

日本国特許庁

JAPAN PATENT OFFICE

K. Nadehara

1/27/04

Q79582

10f1

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2003年 1月28日

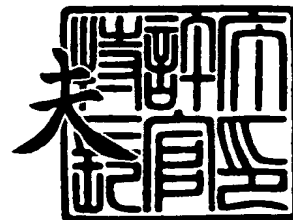
出願番号  
Application Number: 特願2003-018845  
[ST. 10/C]: [JP2003-018845]

出願人  
Applicant(s): 日本電気株式会社

2003年10月 2日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2003-3081314

【書類名】 特許願  
【整理番号】 34403229  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 11/10  
H03M 13/00

## 【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日  
本電気株式会社内

【氏名】 撫原 恒平

## 【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

## 【代理人】

【識別番号】 100109313

## 【弁理士】

【氏名又は名称】 机 昌彦

【電話番号】 03-3454-1111

## 【選任した代理人】

【識別番号】 100085268

## 【弁理士】

【氏名又は名称】 河合 信明

【電話番号】 03-3454-1111

## 【選任した代理人】

【識別番号】 100111637

## 【弁理士】

【氏名又は名称】 谷澤 靖久

【電話番号】 03-3454-1111

## 【手数料の表示】

【予納台帳番号】 191928

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213988

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 AES暗号処理装置、AES復号処理装置、および、AES暗号・復号処理装置

【特許請求の範囲】

【請求項1】 ステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を暗号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とするAES暗号処理装置。

【請求項2】 AES暗号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES暗号化命令を実行するAES暗号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とするAES暗号処理装置。

【請求項3】 AES暗号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES暗号化命令、排他的論理和演算命令を実行するAES暗号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論

理和演算を実行する演算器とを有することを特徴とするAES暗号処理装置。

【請求項4】 即値部分が、第0行を指定すると、係数  $\{02\}$  ,  $\{01\}$  ,  $\{01\}$  ,  $\{03\}$  を出力し、第1行を指定すると、係数  $\{03\}$  ,  $\{02\}$  ,  $\{01\}$  ,  $\{01\}$  を出力し、第2行を指定すると、係数  $\{01\}$  ,  $\{03\}$  ,  $\{02\}$  ,  $\{01\}$  を出力し、第3行を指定すると、係数  $\{01\}$  ,  $\{01\}$  ,  $\{03\}$  ,  $\{02\}$  を出力する前記係数テーブルを有することを特徴とする請求項2、または、請求項3記載のAES暗号処理装置。

【請求項5】 ステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を復号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とするAES復号処理装置。

【請求項6】 AES復号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES復号化命令を実行するAES復号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とするAES復号処理装置。

【請求項7】 AES復号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES復号化命令、排他的論理和演算命令を実行するAES復号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力

する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とするAES復号処理装置。

【請求項8】 即値部分が、第0行を指定すると、係数  $\{0e\}$  ,  $\{09\}$  ,  $\{0d\}$  ,  $\{0b\}$  を出力し、第1行を指定すると、係数  $\{0b\}$  ,  $\{0e\}$  ,  $\{09\}$  ,  $\{0d\}$  を出力し、第2行を指定すると、係数  $\{0d\}$  ,  $\{0b\}$  ,  $\{0e\}$  ,  $\{09\}$  を出力し、第3行を指定すると、係数  $\{09\}$  ,  $\{0d\}$  ,  $\{0b\}$  ,  $\{0e\}$  を出力する前記係数テーブルを有することを特徴とする請求項6、または、請求項7記載のAES復号処理装置。

【請求項9】 ステートの1要素を取り出す第1の選択手段と、前記第1の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第1の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第2の選択手段と、前記第2の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第3の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第3の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とするAES暗号・復号処理装置。

【請求項10】 AES暗号化命令、AES復号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES暗号化命令、AES復号化命令を実行するAES暗号・復号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す第1の選択手段と、前記第1の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第1の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第2の選択手段と、前記第

2 の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第 3 の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第 3 の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第 2 オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とする AES 暗号・復号処理装置。

【請求項 11】 AES 暗号化命令、AES 復号化命令であることを示す部分、入力レジスタを指定する第 1 オペランド部分、出力レジスタを指定する第 2 オペランド部分、行を指定する即値部分を含む AES 暗号化命令、AES 復号化命令を実行する AES 暗号・復号処理装置であって、第 1 オペランド部分、即値部分にしたがい前記入力レジスタからステートの 1 要素を取り出す第 1 の選択手段と、前記第 1 の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第 1 の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第 2 の選択手段と、前記第 2 の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第 3 の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第 3 の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第 2 オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とする AES 暗号・復号処理装置。

【請求項 12】 前記第 1 の選択手段、前記逆アフィン変換回路、前記第 2 の選択手段、前記逆数換字テーブル、前記アフィン変換回路、第 3 の選択手段を多重化し、複数列を同時に処理することを特徴とする請求項 10、または、請求項 11 記載の AES 暗号・復号処理装置。

【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、AES暗号処理装置、AES復号処理装置、および、AES暗号・復号処理装置に関し、特に、所要テーブル容量を削減したAES暗号処理装置、AES復号処理装置、および、AES暗号・復号処理装置に関する。

## 【0002】

## 【従来の技術】

光ファイバ、ADSL、CATVなど安価なブロードバンド・インターネット・アクセス手段の普及にともない、インターネット上に暗号で保護された仮想的な通信チャネル（Virtual Private Network, VPN）を用意して高価な専用線を代替し、通信費用の削減を図る動きが加速しつつある。

## 【0003】

現在VPNに用いられている暗号は、56bit長の共通鍵を用いる米国標準暗号（Data Encryption Standard, DES）やその拡張である3DESである。しかし、今後は、3DESと同等の演算量でより暗号強度が強いと言われている次期米国標準暗号AES（Advanced Encryption Standard）暗号に置き換えられていくと思われる。たとえば、企業の本支店など遠隔地にあるネットワーク間をVPNで結ぶルータにAES暗号化機能を実装する方法としては、AES専用ハードウェア・アクセラレータを内蔵する、内蔵マイクロプロセッサに暗号処理専用命令を追加するなどいくつか考えられるが、いずれの場合でも、構成要素として小型かつ高速なAES処理回路が必要となる。

## 【0004】

以下、AES暗号の概要と従来の実装例を説明する。まず、図21～図26を用い、米国の連邦情報処理規格（Federal Information Processing Standards Publication, FIPS）197（非特許文献1、以下、FIPS197と記す）で規定されているAESの暗号化手順を説明する。



## 【0005】

AESで用いられるデータ構造である「ステート」を図21に示す。AESでは、入力データを128ビット単位のブロックに区切り、128, 192, 256ビット長の共通鍵で暗号化する。128ビット入力は、16個のバイト(8ビット)データに分解され、4行4列の配列に格納される。この配列を「ステート」と呼ぶ。入力データに対する操作は全てこのステート上で行われる。入力ブロック中の各バイトを早い順に $i_{n0}$ から $i_{n15}$ で表すと、図21(a)に示すように、連続したバイトは同一列に格納される。以下の説明では、ステート上の第 $i$ 行 $j$ 列の要素を、 $S_{i,j}$  ( $0 \leq i, j \leq 3$ )と表す(図21(b))。

## 【0006】

AESの暗号化処理は非特許文献1(FIPS197, Figure 5)に疑似コードで示されているが、これをフローチャート化したものを図22に示す。図22に示すように、AES暗号化では、「ラウンド(1403)」と呼ばれるひとまとまりの処理を繰り返すことで暗号化する。ラウンドの回数( $N_r$ )は鍵長により決まり、鍵長が128, 192, 256ビット時のラウンドの回数はそれぞれ10, 12, 14回である。原則としてラウンドはSubBytes(1404, バイト置換)、ShiftRows(1405, 同一行内のシフト), MixColumns(1406, 同一列内の相互演算), AddRoundKey(1407, 拡大鍵の加算)から構成される。ただし、第1ラウンドの前にもAddRoundKeyがあり(1402)、最終ラウンド1408にMixColumnsはない。以下単に「ラウンド」と表記するときは、最終ラウンド以外のラウンドを指すこととする。

## 【0007】

ラウンドを構成する各処理について説明する。SubBytes 1404は、ステート上の各要素を1バイト入出力の換字テーブルにより1対1に変換する処理である。8ビット256語の換字テーブルの内容は、非特許文献1(FIPS197, Figure 7)で与えられているが、数学的には、入力値のガロア体 $GF(2^8)$ 上の逆数を取り、その結果にビット間の排他的論理和によるアフィン変換(非特許文献1(FIPS197, 式(5.1)、または、式(5.2))

”)を施した結果を予め計算しておいたものである。以下、この換字テーブルを、非特許文献1 (FIPS197, Figure 7) のキャプションにならい `ShiftRows1405` と記す。`ShiftRows1405` は、同一行内のシフト処理である。第  $i$  行 ( $0 \leq i \leq 3$ ) の4要素を  $i$  要素左ローテイト処理する。`MixColumns1406` では、非特許文献1 (FIPS197, 式(5.6)) で与えられている係数を用い、同一行内で積和演算(乗算と加算)処理を行う。`AddRoundKey1407` は、共通鍵から生成した拡大鍵を加算する。ここで、`MixColumns` で用いる乗算と加算、`AddRoundKey` で用いる加算は、ガロア体  $GF(2^8)$  上で8ビットの数値間に定義された演算を用いる。ガロア体  $GF(2^8)$  上の加算はビットごとの排他的論理和で行えるため加算器はゲート数個で構成できるが、ガロア体乗算器を構成するには数十ゲート必要である。

#### 【0008】

ラウンドを構成する処理のうち、`SubBytes1404`, `ShiftRows1405`, `MixColumns1406` 処理を高速化する従来の技術を説明する。これら3つの処理に注目するのは、`SubBytes` は、テーブル参照を多く含み、また `MixColumns` は、ガロア体  $GF(2^8)$  上の乗算を多く含むために実装方法によっては演算量を要求すること、また `ShiftRows` は `SubBytes` と一体化して処理できることによる。一方、`AddRoundKey` は単純であり独立性が高いので、別に処理しても問題がない。

#### 【0009】

`SubBytes`, `ShiftRows`, `MixColumns` 処理を一体化したシグナルフローを図23に示す。この図には、ステートを構成する16要素のうち、1列分4要素のラウンド処理結果を出力するためのシグナルフローを示してある。従って、ステートの全16要素(4列)について1ラウンド分の結果を得るには、図23に示したのと同等の演算を、ステート上の入出力位置をシフトしながら合計4回繰り返す必要がある。なお、図23において、`SubBytes1501` と `ShiftRows` との処理順序は入れ替えてある。`SubBytes` は場所を保存したまま値を変える処理、`ShiftRows` は値を保存し

たまま場所を変える処理なので、順序を入れ替えても同一の結果が得られる。また、Shift Rowsは、Sub Bytesの各入力の取得位置を指定する操作で実現されている。Mix Columnsでは、各S-box出力に個別に係数を乗算1502したうえで加算1503する。係数の値は、非特許文献1 (FIPS 197, 式(5.6)) に示された通りである。ここで、GF(2<sup>8</sup>)上の係数との乗算であることを明示するため、非特許文献1 (FIPS 197, 4章) での記述にならない「 $\cdot \{16進数\}$ 」と表記してある。

#### 【0010】

次に、AESラウンド処理の高速ハードウェア実装手法について説明する。

#### 【0011】

従来の高速化手法としては、複数のS-boxを用意し並列処理することが行われてきた。たとえば、非特許文献2では、同一内容のS-boxを16個用意し、ステートの全16要素を同時に処理している。類似例では、非特許文献3でも、AESに選定されたRijndaelのデータブロック長128ビット・モードにおいては、同一内容のS-boxを16個用意し、ステート上の全16要素を同時に処理している。

#### 【0012】

さらに、並列度を上げた例として、非特許文献4がある。非特許文献4において、McLooneらは、ステートの全16要素分、かつ128ビット鍵時の全10ラウンド分のハードウェアを用意し並列処理しているが、そこから図23に対応する1ラウンド4要素分のSub Bytes, Shift Rows, Mix Columns処理回路を抜き出したものを図24に示す。図24に示したように、S-boxの内容を定数倍する代わりに予め係数倍した内容を格納したS-boxを係数の種類だけ用意し、ガロア体乗算器1502を不要としている。具体的には、S-box出力を $\{02\}$ ,  $\{03\}$ 倍する代わりに、S-boxをそのまま実装したテーブルに加え、S-boxテーブル上の各値を $\{02\}$ ,  $\{03\}$ 倍した値を格納したテーブルも用意している。

#### 【0013】

このように、既存のハードウェア実装ではS-boxの容量を増やすことで並

“列度を上げ、高速化を図ってきた。

【0014】

次に、大容量テーブルを使ったAESラウンド処理の高速ソフトウェア実装手法について説明する。

【0015】

非特許文献5に、市販マイクロプロセッサ上のアセンブリ言語でAESを実装したソースコード例 `aescript.asm` がある。ここでは、図25に示すシグナルフロー図に従った演算が行われている。

【0016】

この手法では、8ビット256語の `S-box` (1501, 1601) の代わりに、32ビット256語の拡張 `S-box0`, 拡張 `S-box1`, 拡張 `S-box2`, 拡張 `S-box3` を予め計算し主記憶上に保持しておく (1701)。テーブル中のすべての語について、拡張 `S-box0` ではビット0～7, 8～15, 16～23, 24～31に、同じインデックス位置の `S-box` テーブル値をそれぞれ {02}, {01}, {01}, {03} 倍した値を格納しておく。同様にテーブル各出力の、ビット0～7, 8～15, 16～23, 24～31に、同じインデックス位置の `S-box` 値を、拡張 `S-box1` ではそれぞれ {03}, {02}, {01}, {01} 倍した値を、拡張 `S-box2` ではそれぞれ {01}, {03}, {02}, {01} 倍した値を、拡張 `S-box3` ではそれぞれ {01}, {01}, {03}, {02} 倍した値を格納しておく。このような拡張 `S-box0`～3を用意すれば、4回の拡張 `S-box` 読み出し1702と、4回のGF(2<sup>8</sup>)上の加算1703で図23と同等のシグナルフローが実現でき、1ラウンド1列(4要素)分の `SubBytes`, `ShiftRows`, `MixColumns` 処理が行える。

【0017】

非特許文献5の方法 (Gladmanの方法) は、1個の32ビット長レジスタに8ビット長の要素を4個パックして4並列SIMD (Single Instruction Multiple Data) 演算を行うため高速である。

【0018】

最後に、AES復号化について述べる。

#### 【0019】

AES復号化は、非特許文献1（FIPS197, Figure15）に疑似コードで示されているが、これをフローチャート化したものを図26に示す。

#### 【0020】

ここで、InvSubBytes1804は、SubBytes1404の逆処理、InvShiftRows1805は、ShiftRows1405の逆処理、InvMixColumns1806は、MixColumns1406の逆処理である。AddRoundKey1407の逆処理はAddRoundKey自身であるが、区別のためAddRoundKey'1807と表記してある。

#### 【0021】

復号化は、単純に暗号化の逆処理である。ただし、図26に示した復号化では、図22に示した暗号化の各処理を逆順に行うだけでなく、次に述べるように処理順序の最適化を施している。まず、InvShiftRows1805とInvSubBytes1804とを入れ替えている。InvShiftRows1805は、値を保ったまま場所を変える処理であり、InvSubBytes1804は、場所を保ったまま値を変える処理なので、順番を入れ替えても結果は同一である。

#### 【0022】

次に、AddRoundKey'1807とInvMixColumns1806を入れ替えている。InvMixColumns1806は、線形処理なので、本来、AddRoundKey'1807の出力に、InvMixColumns1806を施すべきところ、InvMixColumns1806の出力に、AddRoundKey'1807を施しても同一の結果が得られる。

#### 【0023】

ただし、順序を入れ替えたAddRoundKey'1807では、暗号化時と同じ拡大鍵ではなく、InvMixColumns1806を施した拡大鍵を使う必要がある。

**【0024】**

AES暗号化処理のフローチャート図22と復号化処理のフローチャート図26を比較すると、ラウンド内の処理は暗号化と復号化で良く似ていることがわかる。違いはSubBytes1404とInvSubBytes1804で用いる換字テーブルの内容とMixColumns1406とInvMixColumns1806で用いる係数である。InvSubBytes1804ではFIPS197, Figure14で示されている換字テーブル（以下InverseS-box）を、InvMixColumns1806ではFIPS197, 式(5.10)で与えられている係数を用いる。

**【0025】**

AES復号化の実装を説明する。暗号化と復号化のフローチャートは似ているので、図24に示したMcLooneらの方法を復号化のうちInvSubBytes1804, InvShiftRows1805, InvMixColumns1806の高速処理に適用できる。この場合、1ラウンド1列あたりInvS-boxの内容を{09}, {0b}, {0d}, {0e}倍した4種類のテーブルを要素ごとに用意する、すなわち8ビット256語のテーブルを1列あたり16個、1ラウンド1要素あたりに換算して4個(8Kビット)使用する。これらの復号化に用いるテーブルは、暗号化とは共用できない。

**【0026】**

図25に示したGladmanの方法も復号化InvSubBytes1804, InvShiftRows1805, InvMixColumns1806の高速処理に適用できる。この場合、暗号化と同様、復号化でも1ラウンド1列あたり32ビット256語のテーブルを4個(32kビット)用意しなければならない。これらの復号化に用いるテーブルは、暗号化とは共用できない。

**【0027】**

また、ガロア体上の演算器を利用する技術としては、特許文献1記載の技術がある。

**【0028】****【特許文献1】**

特開 2000-322280 号公報

【非特許文献 1】

連邦情報処理規格 (Federal Information Processing Standards Publication)、FIPS 197、(米国)

【非特許文献 2】

清家秀律ほか、「FPGA を用いた AES 暗号の試作」、電子情報通信学会技術報告、VLD2001-91, ICD2001-35, FTS2001-38, 2001 年 11 月

【非特許文献 3】

Patrick R. Schaumont ほか、“Unlocking the Design Secrets of a 2.29 Gb/s Rijndael Processor”, Proc. 39th Design Automation Conference, 講演番号 41.1, June 2002

【非特許文献 4】

M. McLoone ほか、“Rijndael FPGA Implementation Utilizing Look-Up Tables”, IEEE Workshop on Signal Processing Systems, 2001 年, p. 349~p. 360

【非特許文献 5】

Brian Gladman、ソフトウェア・アーカイブ aessrc.zip、[online]、[平成 15 年 1 月 10 日検索]、インターネット<[http://fp.gladman.plus.com/cryptography\\_technology/rijndael/](http://fp.gladman.plus.com/cryptography_technology/rijndael/)>

【0029】

【発明が解決しようとする課題】

非特許文献 2 の方法では、暗号化のために 1 ラウンドあたり 8 ビット 256 語のテーブル 16 個、計 32 k ビットを用意し、ステート上の全 16 要素を同時に

計算している。1 ラウンド 1 要素あたりに換算すれば 2 k ビットのテーブルを使用している。

#### 【0030】

非特許文献 4 の方法では、暗号化のために 1601 のようにステート 1 列あたり 8 ビット 256 語のテーブルを 12 個 (24 k ビット)、1 ラウンド 1 要素あたりに換算して 3 個 (6 k ビット) 使用している。復号化のためには 8 ビット 256 語のテーブルを 16 個 (32 k ビット)、1 ラウンド 1 要素あたりに換算して 4 個 (8 k ビット) 使用する。

#### 【0031】

非特許文献 5 の方法では、暗号化のために、32 ビット 256 語のテーブルを 4 個 (32 k ビット) 用意する必要がある。1 ラウンド 1 要素あたりに換算すれば、8 k ビット使用している。復号化のためにも同じく 32 ビット 256 語のテーブルを 4 個 (32 k ビット)、1 ラウンド 1 要素あたりに換算すれば、8 k ビットのテーブルを用意する必要がある。

#### 【0032】

このように、従来の技術では、処理に用いるテーブル容量を増やすことで高速化を図ってきた。しかし、テーブル容量の増加は AES 演算器のハードウェア規模の増大に直結する。たとえば、非特許文献 4 の方法では、ガロア体乗算器を削除する代わりに、S-box テーブルの個数を増やしているが、ガロア体乗算器は、数十ゲート規模で構成できるのに対し、8 ビット 256 語の S-box テーブルは、数千～1 万ゲート規模もあるため、高速化の代償としてハードウェア規模が飛躍的に増えている。しかし、高速化は重要だが、ハードウェア規模が増大するのでは実用的とはいえない。

#### 【0033】

同様、特許文献 1 にも、効果的なハードウェア量削減の技術は、開示されていない。

#### 【0034】

本発明の目的は、処理性能を保ちつつ、S-box テーブル容量を削減した、小型かつコストパフォーマンスの良い AES 暗号処理装置を実現することである



## 【0035】

## 【課題を解決するための手段】

本発明の第1のAES暗号処理装置は、ステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を暗号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とする。

## 【0036】

本発明の第2のAES暗号処理装置は、AES暗号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES暗号化命令を実行するAES暗号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とする。

## 【0037】

本発明の第3のAES暗号処理装置は、AES暗号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES暗号化命令、排他的論理和演算命令を実行するAES暗号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガ

“ ロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とする。

#### 【0038】

本発明の第4のAES暗号処理装置は、前記第2、または、第3のAES暗号処理装置であって、即値部分が、第0行を指定すると、係数  $\{02\}$  ,  $\{01\}$  ,  $\{01\}$  ,  $\{03\}$  を出力し、第1行を指定すると、係数  $\{03\}$  ,  $\{02\}$  ,  $\{01\}$  ,  $\{01\}$  を出力し、第2行を指定すると、係数  $\{01\}$  ,  $\{03\}$  ,  $\{02\}$  ,  $\{01\}$  を出力し、第3行を指定すると、係数  $\{01\}$  ,  $\{01\}$  ,  $\{03\}$  ,  $\{02\}$  を出力する前記係数テーブルを有することを特徴とする。

#### 【0039】

本発明の第1のAES復号処理装置は、ステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を復号化用に変換する換字テーブルと、選択された要素の行に応じた係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とする。

#### 【0040】

本発明の第2のAES復号処理装置は、AES復号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES復号化命令を実行するAES復号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とする。

#### 【0041】

本発明の第3のAES復号処理装置は、AES復号化命令であることを示す部

分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES復号化命令、排他的論理和演算命令を実行するAES復号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタから状態の1要素を取り出す選択手段と、前記選択手段により取り出された要素を変換する換字テーブルと、即値部分にしたがい4個の係数を出力する係数テーブルと、前記換字テーブルの出力と前記係数テーブルからの各係数とを乗算し、連結して出力するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とする。

#### 【0042】

本発明の第4のAES復号処理装置は、前記第2、または、第3のAES復号処理装置であって、即値部分が、第0行を指定すると、係数 {0e} , {09} , {0d} , {0b} を出力し、第1行を指定すると、係数 {0b} , {0e} , {09} , {0d} を出力し、第2行を指定すると、係数 {0d} , {0b} , {0e} , {09} を出力し、第3行を指定すると、係数 {09} , {0d} , {0b} , {0e} を出力する前記係数テーブルを有することを特徴とする。

#### 【0043】

本発明の第1のAES暗号・復号処理装置は、状態の1要素を取り出す第1の選択手段と、前記第1の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第1の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第2の選択手段と、前記第2の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第3の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第3の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を連結して累算するガロア体加算器とを有することを特徴とする。

#### 【0044】

本発明の第2のAES暗号・復号処理装置は、AES暗号化命令、AES復号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES暗号化命令、AES復号化命令を実行するAES暗号・復号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す第1の選択手段と、前記第1の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第1の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第2の選択手段と、前記第2の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第3の選択手段と、選択された要素の行に応じた係数を出力する係数テーブルと、前記第3の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段とを有することを特徴とする。

#### 【0045】

本発明の第3のAES暗号・復号処理装置は、AES暗号化命令、AES復号化命令であることを示す部分、入力レジスタを指定する第1オペランド部分、出力レジスタを指定する第2オペランド部分、行を指定する即値部分を含むAES暗号化命令、AES復号化命令を実行するAES暗号・復号処理装置であって、第1オペランド部分、即値部分にしたがい前記入力レジスタからステートの1要素を取り出す第1の選択手段と、前記第1の選択手段により取り出された要素を逆アフィン変換する逆アフィン変換回路と、暗号化の場合には前記第1の選択手段の出力を選択し、復号化の場合には前記逆アフィン変換回路の出力を選択する第2の選択手段と、前記第2の選択手段の出力を暗号化・復号化用に変換する逆数換字テーブルと、前記逆数換字テーブルの出力をアフィン変換するアフィン変換回路と、暗号化の場合には前記アフィン変換回路の出力を選択し、復号化の場合には前記逆数換字テーブルの出力を選択する第3の選択手段と、選択された要

素の行に応じた係数を出力する係数テーブルと、前記第3の選択手段の出力と前記係数テーブルからの各係数とを乗算するガロア体乗算器と、前記ガロア体乗算器の出力を第2オペランド部分で指令された出力レジスタに格納する格納手段と、排他的論理和演算を実行する演算器とを有することを特徴とする。

#### 【0046】

本発明の第4のAES暗号・復号処理装置は、前記第2、または、第3のAES暗号・復号処理装置であって、前記第1の選択手段、前記逆アフィン変換回路、前記第2の選択手段、前記逆数換字テーブル、前記アフィン変換回路、第3の選択手段を多重化し、複数列を同時に処理することを特徴とする。

#### 【0047】

##### 【発明の実施の形態】

AESでは、ガロア体 (Galois field, GF) 上の演算を、アルゴリズムの定義に用いている。

#### 【0048】

まず、GF(2<sup>8</sup>) 上の数について説明する。

#### 【0049】

一般に、GF(p) 上の元を係数とするm次の多項式は、既約多項式 (irreducible polynomial) を法とする加算と乗算について体をなし、この体をGF(p<sup>m</sup>) と表記する。GF(2<sup>8</sup>) 上の多項式は、一般に次のように書ける。

#### 【0050】

$$b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0 \quad (1)$$

#### 【0051】

ここで、 $b_i$  ( $0 \leq i \leq 7$ ) は、ガロア体GF(2) 上の要素なので、0か1である。式(1)は、係数のみ取り出し  $\{b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0\}$  とベクトル表現でも書ける。かっこ内部を16進表記することもある。

#### 【0052】

GF(2<sup>8</sup>) 上には30個余りの既約多項式があるが、AESでは次式(2)

"を採用している。

【0053】

$$m(x) = x^8 + x^4 + x^3 + x + 1 \quad (2)。$$

【0054】

次に、AESにおけるGF(2<sup>8</sup>)上の加算について説明する。

【0055】

GF(2<sup>8</sup>)上の加算は、ベクトル表現された数のビットごとの排他的論理和(XOR)をとるだけでよい。すなわち、 $\{a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0\}$ と $\{b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0\}$ との和 $\{c_7 c_6 c_5 c_4 c_3 c_2 c_1 c_0\}$ は次式(3)で表される。多項式の加算は、同次数の係数どうしを加算すればよく、GF(2)上の加算は排他的論理和(XOR)だからである。ここで、<XOR>は、排他的論理和を示す。

【0056】

$$c_i = a_i <XOR> b_i \quad (0 \leq i \leq 7) \quad (3)。$$

【0057】

図13は、ガロア体GF(2<sup>8</sup>)上の加算器の例を示すブロック図である。

【0058】

図13を参照すると、ハードウェアによるGF(2<sup>8</sup>)上の加算器は、XORゲート8個で簡単に構成できる。通常の2進数とは異なり、桁上げ処理は不要である。

【0059】

次に、AESにおけるGF(2<sup>8</sup>)上の乗算について説明する。

【0060】

図14は、ガロア体GF(2<sup>8</sup>)上の2倍回路の例を示すブロック図である。

【0061】

乗算は、被乗数の2のべき乗倍と加算の組み合わせで実現する。まず、入力を2倍する方法を説明する。式(1)を $2 = \{00000010\}$ 倍することは、 $x$ 倍することに等しいので、次式(5)で表せる。これは、ベクトル表現を左1bitシフトすることに等しい。

## 【0062】

$b_7 x^8 + b_6 x^7 + b_5 x^6 + b_4 x^5 + b_3 x^4 + b_1 x^3 + b_1 x^2 + b_0 x^1$  (5)。

## 【0063】

次に、この式(5)を、式(2)で定義した $m(x)$ に対して既約にする。 $b_7 = 0$ ならば既約であるが、 $b_7 = 1$ の場合は既約ではないので、式(5)から $m(x)$ を減算する、すなわち、 $\{1b\} = \{00011011\}$ とXORする必要がある。この一連の操作は、たとえば、図14に示した回路で行える。

## 【0064】

任意の数との乗算は、部分積を発生する2倍回路とANDゲート、部分積を加算する回路の組み合わせで実現できる。

## 【0065】

図15は、ガロア体 $GF(2^8)$ 上のガロア体乗算器の例を示すブロック図である。

図15において、「 $2\times$ 」は、図14の2倍回路を示す。また、「XOR」は、図13の加算器である。実装方法にもよるが、暗号化時は $\{02\}$ 、 $\{03\}$ 倍の回路が必要になる。復号化時は $\{09\}$ 、 $\{0b\}$ 、 $\{0d\}$ 、 $\{0e\}$ 倍の回路が必要になる。

## 【0066】

次に、本発明の第1の実施の形態について図面を参照して詳細に説明する。

## 【0067】

図1は、本発明の第1の実施の形態の構成を示すブロック図である。

## 【0068】

図1を参照すると、本発明の第1の実施の形態は、入力ステート101と、列マルチプレクサ102と、演算入力レジスタ103と、行マルチプレクサ104と、S-boxテーブル105と、係数テーブル106と、ガロア体 $GF(2^8)$ 上のガロア体乗算器107と、演算結果レジスタ108と、ガロア体加算器109と、累算レジスタ110とから構成されるAES暗号化装置である。また、演算入力レジスタ103、行マルチプレクサ104、S-boxテーブル

105、係数テーブル106、ガロア体GF(2<sup>8</sup>)上のガロア体乗算器107、および、演算結果レジスタ108を含む部分をAES暗号回路111とする。

#### 【0069】

ガロア体GF(2<sup>8</sup>)上のガロア体乗算器107は、図15に示すものであり、図15のb<sub>7</sub>～b<sub>0</sub>には、S-boxテーブル105の出力8ビットが入力され、a<sub>1</sub>～a<sub>0</sub>には、係数テーブル106の出力2ビット（たとえば、図2の行指定0の整数1の{01}を示す2ビット“01”）が接続される。a<sub>7</sub>～a<sub>2</sub>の部分の回路は、設けなくてよい。ガロア体GF(2<sup>8</sup>)上のガロア体乗算器107には、図15の乗算器が4個設けられる。

#### 【0070】

演算入力レジスタ103、演算結果レジスタ108は、遅延時間、パイプライン制御等を考慮したものであり、必ずしも必要はない。

#### 【0071】

入力ステート101は、S<sub>0</sub>, 0～S<sub>3</sub>, 3の16個の要素（データ）であり、それぞれの要素は、8ビットである。また、たとえば、入力ステート101の1列ずつが、ソフトウェア可視のレジスタに格納される。

#### 【0072】

列マルチプレクサ102は、4列ある入力ステート101から指定された1列4要素を選択し出力する。演算入力レジスタ103は、列マルチプレクサ102の出力である1列4要素を保持する。行マルチプレクサ104は、入力レジスタ103の4要素から指定された行にある1要素（8ビット）を選択し出力する。S-boxテーブル105は、行マルチプレクサ104の出力（8ビット）をインデックスとして8ビットのデータを出力する。S-boxテーブル105は、たとえば、256語×8ビットのROM、RAM、または、組み合わせ回路等で構成される。

#### 【0073】

S-boxテーブル105の出力は、GF(2<sup>8</sup>)上のガロア体乗算器107（4個の部分乗算器を含む）に入力される。各部分乗算器には、行指定に従って、係数テーブル106から係数が供給され、GF(2<sup>8</sup>)上の乗算が実行される。



。演算結果レジスタ108は、 $GF(2^8)$ 上のガロア体乗算器107の出力の連結された $4 \times 8$ ビットのデータを格納する。ガロア体加算器109は、演算結果レジスタ108の $4 \times 8$ ビットの値と累算レジスタ110上の値との $GF(2^8)$ 上の加算を実行する。累算レジスタ110は、ガロア体加算器109の出力( $4 \times 8$ ビット)を格納する。このようにして、ステート1列分のSubBytes, ShiftRows, MixColumns処理のうち $1/4$ (1要素分)が完了する。

#### 【0074】

図16は、図1のS-boxテーブル105の内容を示す説明図である。

#### 【0075】

図16を参照すると、S-boxテーブル105の内容は、非特許文献1(FIPS197, Figure 7)に示されているものであり、たとえば、インデックスが、{b3}であれば、内容は、{6d}である。

#### 【0076】

図2は、図1の係数テーブル106の内容を示す説明図である。

#### 【0077】

図2を参照すると、係数テーブル106の内容は、非特許文献1(FIPS197, 式(5.6))に示される係数行列を転置したものである。

#### 【0078】

次に、本発明の第1の実施の形態の動作について図面を参照して詳細に説明する。

#### 【0079】

図3は、本発明の第1の実施の形態の動作を示す説明図である。

#### 【0080】

図3を参照すると、事前に累算レジスタ110をゼロクリアしておく(図3S301)。まず、第0列、第0行を処理する。列マルチプレクサ102はステート101から第0列を選択、出力する(図3S302)。その中から行マルチプレクサ104は、第0行の $S_{0,0}$ を選択、出力する(図3S303)。 $S_{0,0}$ をS-boxテーブル105により変換した結果を $S'_{0,0}$ とする(図3

S 3 0 4) 。 S' ' 0, 0 を係数テーブル 1 0 6 の第 0 行の 4 個の出力と乗算し、連結して出力する (図 3 S 3 0 5) 。 4 バイト長のガロア体乗算器 1 0 7 の出力は、累算レジスタ 1 1 0 の内容に加算される (図 3 S 3 0 6) 。

#### 【0081】

同様に、第 1 列第 1 行 S<sub>1, 1</sub>、第 2 列第 2 行 S<sub>2, 2</sub>、第 3 列第 3 行 S<sub>3, 3</sub> も順次処理する。列マルチプレクサ 1 0 2 は、入力ステート 1 0 1 から、それぞれ、第 1, 2, 3 列を選択、出力する。その中から、行マルチプレクサ 1 0 4 は、それぞれ、第 1 行の S<sub>1, 1</sub>、第 2 行の S<sub>2, 2</sub>、第 3 行の S<sub>3, 3</sub> を選択、出力する。S<sub>1, 1</sub>、S<sub>2, 2</sub>、S<sub>3, 3</sub> をそれぞれ S-box テーブル 1 0 5 により変換した結果を S' ' 1, 1, S' ' 2, 2, S' ' 3, 3 とし、それぞれ係数テーブル 1 0 6 の第 1, 2, 3 行の 4 個の出力と乗算し、連結して出力する。4 バイト長のガロア体乗算器 1 0 7 の出力は、累算レジスタ 1 1 0 の内容にガロア体加算機 1 0 9 により加算される。ガロア体乗算器 1 0 7 からの第 3 行の出力を累算レジスタ 1 1 0 に加算し終わると、累算レジスタ 1 1 0 に、1 列 4 要素分の Sub Bytes, Shift Rows, Mix Columns 結果が得られる (図 3 S 3 0 7) 。この得られた結果は、図 2 5 示す非特許文献 5 の方法 (Gladman の方法) の結果に等しい。

#### 【0082】

本発明の第 1 の実施の形態の特長は、図 2 5 に示した非特許文献 5 (Gladman) の方法における拡張 S-box 1 7 0 1 と同等の出力を得るために必要なハードウェア量を約 1 / 1 6 に削減した点にある。図 2 5 に示した方法では、3 2 ビット 2 5 6 語のテーブルを 4 種類、計 3 2 k ビットのハードウェア資源が必要である。一方、図 1 に示した本発明の方法では、8 ビット 2 5 6 語の 1 個の S-box テーブル 1 0 5 (計 2 k ビット) とガロア体乗算器 1 0 7 とで同等の出力が得られる。

#### 【0083】

8 ビット 2 5 6 語の S-box テーブル 1 0 5 の規模は数千～1 万ゲートあり、これと比較して 1 個あたり数十ゲート規模でしかないガロア体乗算器 1 0 7 のコストは無視できるため、必要なハードウェア量は S-box テーブル 1 0 5 の

容量に比例するとしてよい。したがって、2kビットのS-boxテーブル105を使う本発明の第1の実施の形態は、32kビットのテーブルを使う非特許文献5（Gladman）の方法に比べ、1/16のハードウェア規模で同等の演算が行える効率の良い方法といえる。

#### 【0084】

以上、本発明の第1の実施の形態によれば、AES暗号化に必要なハードウェア量を大幅に削減できることを示した。その理由は、本発明の第1の実施の形態では、拡張S-box1701の内容を全て予め計算しておく非特許文献5（Gladman）の方法とは異なり、小さなS-boxテーブル105と小規模な演算器群とを組み合わせ実行時に値を生成しているからである。

#### 【0085】

次に、本発明の第2の実施の形態について図面を参照して詳細に説明する。

#### 【0086】

図4は、本発明の第2の実施の形態の構成を示すブロック図である。

#### 【0087】

図5は、AES暗号化専用命令のニーモニック表記例を示す説明図である。

#### 【0088】

図6は、入力レジスタrs、出力レジスタrtのデータ配置を示す説明図である。

#### 【0089】

図7は、AES暗号化命令の即値と出力との関係を示す説明図である。

#### 【0090】

本発明は、非特許文献5（Gladman）のソフトウェア向けアルゴリズムと同等のシグナルフローを実現しているので、マイクロプロセッサのAES暗号化専用命令により本発明を利用してAES暗号の符号化、復号化の実行させることができる。本発明の第2の実施の形態は、マイクロプロセッサにAES暗号化専用命令を追加し、図1に示した本発明の第1の実施の形態を演算器として利用し、AES暗号化処理を実施するものである。

#### 【0091】

図5に示すように、AES暗号化命令の名称は説明文中で参照する都合上、たとえば、“AES\_SSM (AES Sub Bytes, Shift Rows, Mix Columns)” とする。この命令は入力レジスタ  $r_s$ 、出力レジスタ  $r_t$ 、即値  $imm$  の3個のオペランドをとる。入力レジスタ  $r_s$ 、出力レジスタ  $r_t$  とも、32ビット長以上あり、ステートの要素を1列分4個連結して格納できるものとする。

#### 【0092】

それぞれ、図6 (a) は、入力レジスタ  $r_s$  のデータ配置を、図6 (b) は、出力レジスタ  $r_t$  のデータ配置を示す。図5に示す“AES\_SSM”命令は、入力レジスタ  $r_s$  の即値  $imm$  によって指定された行の1バイトをS-boxテーブル105で変換し (S-box () と表記)、ガロア体乗算器107によるGF(2<sup>8</sup>) 上の乗算により {01} , {02} , または、 {03} 倍し、図7に示す順序で連結して出力レジスタ  $r_t$  に格納する。

#### 【0093】

図4を参照すると、本発明の第2の実施の形態は、レジスタファイル等で構成されるソフトウェア可視の汎用レジスタ  $r_0 \sim r_n$  (“AES\_SSM”命令の  $r_s$ 、 $r_t$  により  $r_0 \sim r_n$  から、入力レジスタ  $r_s$ 、出力レジスタ  $r_t$  が1つずつ指定される) を含む汎用レジスタ群401と、“AES\_SSM”命令コード等が格納される命令バッファ402と、デコーダ403と、補助レジスタ404と、補助レジスタ405と、補助レジスタ406と、補助レジスタ407と、補助レジスタ408と、補助レジスタ409と、XORの演算が可能な汎用演算回路410と、演算結果レジスタ411と、書き込みマルチプレクサ412と、行マルチプレクサ104と、S-boxテーブル105と、係数テーブル106と、ガロア体乗算器107と、演算結果レジスタ108とから構成される。

#### 【0094】

点線で囲まれた部分が、図1のAES暗号回路111にほぼ相当する。補助レジスタ404、補助レジスタ405、補助レジスタ406、補助レジスタ407、補助レジスタ408、補助レジスタ409、演算結果レジスタ411、演算結

果レジスタ 108 は、パイプライン制御のために設けたものであり、必ずしも必要ない。

#### 【0095】

それぞれ 32 ビットであり、入力ステート 101 の 1 列、AES 暗号化命令の結果が格納される。また、汎用レジスタ  $r_0 \sim r_n$  は、入力レジスタ  $r_s$ 、出力レジスタ  $r_t$  に割り当てられる。

#### 【0096】

次に、本発明の実施の第 2 の形態の動作について図面を参照して説明する。

#### 【0097】

図 4 を参照すると、命令バッファ 402 に格納された AES 暗号化命令がデコーダ 403 でデコードされ、 $r_s$  により、汎用レジスタ群 401 から処理される列の格納されている入力レジスタ  $r_s$  の 1 列 4 バイトのデータが選択され行マルチプレクサ 104 に入力される。行マルチプレクサ 104 では、デコーダ 403 からの  $i_{mm}$  (行指定) にしたがって 1 列 4 バイトから 1 バイトのデータが選択され、補助レジスタ 404 に格納される。また、 $i_{mm}$  は、補助レジスタ 405 に格納される。

#### 【0098】

S-box テーブル 105 では、補助レジスタ 404 からの 1 バイトのデータにしたがい 1 バイトのデータが出力され、補助レジスタ 407 に格納される。係数テーブル 106 では、補助レジスタ 405 からの行指定にしたがい図 2 に示す 2 ビット  $\times$  4 ビット、合計 8 ビットの係数が出力され、補助レジスタ 406 に格納される。

#### 【0099】

ガロア体乗算器 107 では、補助レジスタ 407 からの 1 バイトのデータと補助レジスタ 406 からの係数との乗算が実行され、8 ビット  $\times$  4 の乗算結果が演算結果レジスタ 108 に格納される。演算結果レジスタ 108 内の 8 ビット  $\times$  4 の乗算結果は、書き込みマルチプレクサ 412 で選択され、デコーダ 403 からの  $r_t$  にしたがい汎用レジスタ群 401 の出力レジスタ  $r_t$  に格納される。

#### 【0100】

図 8 は、AES\_SSM 命令を用い、SubBytes, ShiftRows, MixColumns を実現する命令列を示す説明図である。

#### 【0101】

ここで、入力状態 101 は、事前に、汎用レジスタ群 401 の汎用レジスタに 1 列ずつ格納されているとする。すなわち、レジスタ  $r_3$  に  $S_{3,3}, S_{2,3}, S_{1,3}, S_{0,3}$  が、レジスタ  $r_2$  に  $S_{3,2}, S_{2,2}, S_{1,2}, S_{0,2}$  が、レジスタ  $r_1$  に  $S_{3,1}, S_{2,1}, S_{1,1}, S_{0,1}$  が、レジスタ  $r_0$  に  $S_{3,0}, S_{2,0}, S_{1,0}, S_{0,0}$  が、この順に上位バイトから下位バイトに向かって格納されているとする。図 8 において、ビットごとの排他的論理和演算命令を XOR と表記する。このとき、1 ラウンド 1 列分の SubBytes, ShiftRows, MixColumns 処理は、図 8 に示す命令列で処理できる。図 1 と比較すると、列マルチプレクサ 102 に対する入力状態 101 の列の指定をその列を収めたレジスタ番号の指定に、ガロア体加算器 109 を排他的論理和演算命令に置き換えることにより、図 1 と同等のシグナルフローを実現している。

#### 【0102】

AES 命令と同様、排他的論理和演算命令は、命令バッファ 402 からデコーダ 403 でデコードされ、汎用レジスタ群 401 の 2 つの汎用レジスタからそれぞれ 4 バイトのデータが読み出され、補助レジスタ 408、補助レジスタ 409 に格納される。汎用演算回路 410 で、補助レジスタ 408 と補助レジスタ 409 からのデータの排他的論理輪演算が実施され、排他的論理輪演算結果の 4 バイトのデータが演算結果レジスタ 411 に格納される。

#### 【0103】

演算結果レジスタ 411 内の 4 バイトの排他的論理輪演算結果は、書き込みマルチプレクサ 412 で選択され、デコーダ 403 から出力にしたがい汎用レジスタ群 401 の 1 つの出力レジスタ  $r_t$  に格納される。

#### 【0104】

図 5 に示した AES 専用命令を導入すれば、AES 暗号化処理は、1 ラウンド 1 列あたり、図 8 に示した 7 命令で処理できる。すなわち、入力状態 101

全体（4列）を処理しても1ラウンドあたり28命令で済む。たとえば128ビット鍵時に必要な全10ラウンド分の処理を、これまで説明を省いたAddRoundKey1407を含めて行っても計300命令程度で済む。従来の非特許文献5（Gladmanの方法）と比較すると、本発明の第2の実施の形態によれば、S-boxテーブル105の容量を1/16と削減しながら、同等の処理速度が達成できる。

#### 【0105】

次に、本発明の第3の実施の形態について図面を参照して詳細に説明する。

#### 【0106】

図9は、本発明の第3の実施の形態で使用する係数テーブル106の内容を示す説明図である。

#### 【0107】

図10は、AES復号化命令の即値と出力との関係を示す説明図である。

#### 【0108】

図17は、Inverse S-boxの内容を示す説明図である。

#### 【0109】

本発明の第3の実施の形態は、AES復号化に関するものである。これらは、図1～図8で説明したAES暗号化処理装置、およびAES暗号化命令と同様に構成できる。

#### 【0110】

AES復号化装置は、図1の係数テーブル106の内容を、非特許文献1（FIPS197、式（5.10））の係数行列を転置したもの（図9）に変更し、S-boxテーブル105の内容を非特許文献1（FIPS197、Figure 14）に示されたInverse S-boxに変更したもの（図17）である。この変更にとともに、AES暗号化装置では係数テーブル106の出力が2ビット×4組であったのに対し、AES復号化装置では係数テーブル106の出力が4ビット×4組になるので、ガロア体乗算器107の各部分乗算器は、8×4ビット構成とする必要もある。

#### 【0111】

AES復号化命令は、図4のうち係数テーブル106の内容を図9に示した非特許文献1(FIPS197, 式(5.10))の係数行列を転置したものに變更し、S-boxの内容を非特許文献1(FIPS197, Figure14)に示されたInverse S-boxに變更したものである。この變更にともない、係数テーブル106の出力が4ビット×4組になるので、ガロア体乗算器107を各8×4ビット構成とする必要もある。AES復号化命令の入出力関係を図10に示す。ここでInvS-box()はInverse S-boxテーブルによる換字を表す。

#### 【0112】

次に、本発明の第4の実施の形態について図面を参照して詳細に説明する。

#### 【0113】

図11は、本発明の第4の実施の形態の構成を示すブロック図である。

#### 【0114】

AES暗号化装置とAES復号化装置は、S-boxおよび係数テーブルの内容が異なり、ガロア体乗算器107のビット幅が異なるだけなので、AES暗号化と復号化の両方が行える装置が容易に構成できる。また、AES暗号化と復号化の両方が行えるAES暗号化・復号化統合命令も容易に構成できる。

#### 【0115】

図11を参照すると、本発明の第4の実施の形態は、図4に示したAES暗号化命令のための演算器と、図9, 図10を参照して説明したAES復号化命令のための演算器を統合し、AES暗号化と復号化の双方に対応させた演算器である。詳細には、逆アフィン変換回路1101と、暗号化マルチプレクサ1102と、逆数テーブル1103と、アフィン変換回路1104と、暗号化マルチプレクサ1105と、行マルチプレクサ104と、係数テーブル106と、ガロア体乗算器107と、演算結果レジスタ108とから構成される。

#### 【0116】

図18は、逆アフィン変換回路1101の内容を示す説明図である。

#### 【0117】

図18を参照すると、 $0 \leq i \leq 7$ であり、 $b_i$ は、入力バイトの第*i*ビット、



$C_i$  は、 $\{05\}$  の第  $i$  ビットであり、 $b'_i$  は、出力の第  $i$  ビットである。＜XOR＞は、排他的論理和である。

#### 【0118】

図19は、逆数テーブル1103の内容を示す説明図である。

#### 【0119】

図20は、アフィン変換回路1104の内容を示す説明図である。

#### 【0120】

図20を参照すると、 $0 \leq i \leq 7$  であり、 $b_i$  は、入力バイトの第  $i$  ビット、 $C_i$  は、 $\{63\}$  の第  $i$  ビットであり、 $b'_i$  は、出力の第  $i$  ビットである。＜XOR＞は、排他的論理和である。

#### 【0121】

非特許文献1（FIPS197，5.1.1節）に記述されているように、暗号化で用いるS-boxテーブル105は入力値のGF(2<sup>8</sup>)上の逆数に、非特許文献1（FIPS197，式(5.1)）に示されるアフィン変換を施したものである。また、復号化で用いるInverseS-boxテーブルは、S-boxテーブル105の逆関数なので、入力値に、非特許文献1（FIPS197，式(5.1)）に示されるアフィン変換の逆変換（以下「逆アフィン変換」）を施した後、GF(2<sup>8</sup>)上の逆数をとったものである。したがって、逆数テーブル1103を1個用意し、暗号化時には、逆数テーブル1103の出力にアフィン変換回路1104による変換を施してS-boxテーブル105と同等の出力を得ることが可能であり、復号化時には、逆数テーブル1103の入力に逆アフィン変換回路1101による変換を施してInverseS-boxテーブルと同等の出力を得ることが可能である。

#### 【0122】

暗号化と復号化の切り替えは、命令語の即値（imm）を1ビット増やして指定することで行える。このビットにしたがい、暗号化マルチプレクサ1102、暗号化マルチプレクサ1105により、暗号化時は逆数テーブル1103の出力にアフィン変換を、復号化時は、逆数テーブル1103の入力に逆アフィン変換を施す。また、このビットは係数テーブル106の出力を、暗号化時は図2に示

した内容を、復号化時は図9に示した内容を入力するよう切り替える。

#### 【0123】

以上、図11を参照しながら、AES暗号化および復号化で共用できる演算器を構成するため、図1、または、図4に施した変更点を説明した。図11に示す本発明の第4の実施の形態によれば、8ビット×256ワード（2kビット）のテーブル1個で、AES暗号化または復号化を4並列で処理できる。

#### 【0124】

従来の技術で説明した非特許文献5（Gladmanの方法）では、暗号化のために32kビットのテーブルを用意する必要があったが、このテーブルは復号化とは共用できず、復号化用にも別に32kビットのテーブルを用意する必要がある。すなわち、非特許文献5（Gladmanの方法）により暗号化と復号化を行おうとすると、計64kビットのテーブルを用意する必要がある。

#### 【0125】

一方、本発明の第4の実施の形態では、同等の演算を2kビットのテーブルで行うため、必要なテーブル容量を1/32まで削減できる。

#### 【0126】

次に、本発明の第2～第4の実施の形態で説明したAES暗号化・復号化命令のバリエーションについて説明する。

#### 【0127】

AES暗号化命令では、図4において、即値が、行マルチプレクサ104、および、係数テーブル106に対し処理対象となる行番号そのものを指定するとしたが、4種類の出力を区別できるなら、図7に示した即値のビットパターンに縛られるものではない。同様の議論はAES復号化命令、AES暗号化・復号化統合命令にも適用可能である。

#### 【0128】

AES暗号化命令が演算対象とする要素のレジスタ上のバイト位置を指定するため、図4では、AES暗号化命令の引数に即値を与えるとしたが、その代わりに命令コードの一部を用いて選択すべき行を指定することもできる。言い換えれば、扱う行別に4種類の命令を用意し、入力レジスタ番号と出力レジスタ番号の

みを引数に与えてもよい。同様の議論は、AES復号化命令、AES暗号化・復号化統合命令にも適用可能である。

#### 【0129】

図5に示したAES暗号化命令では、ロード・ストア・アーキテクチャのマイクロプロセッサを想定したため、入出力データはレジスタファイルで構成される汎用レジスタに置き、命令の引数にレジスタ番号を指定するとしたが、演算の入出力データの片方、または、両方をメモリ上に置けるマイクロプロセッサを想定し、専用命令の引数に何らかのメモリ・アドレス指定を取るよう変更しても、本発明の第2の実施例の本質に影響を与えないため、同様の効果が得られる。同様の議論はAES復号化命令、AES暗号化・復号化統合命令にも適用可能である。

#### 【0130】

図8で示したように、AES暗号化命令の出力に対しXOR命令を発行することが多い。したがって、図4では、AES暗号化命令が、ガロア体乗算器107出力と同等の結果を生成するとしたが、累算レジスタ（図8のr5）も入力に取る3レジスタ命令とし、図1のガロア体加算器109出力と同等の結果を生成するよう変更し、高速化を図ることもできる。同様の議論はAES復号化命令、AES暗号化・復号化統合命令にも適用可能である。

#### 【0131】

図6に示したように、AES暗号化命令、AES復号化命令、AES暗号化・復号化統合命令では、現在、一般的なレジスタ幅が32ビットのマイクロプロセッサを想定したが、レジスタ幅が32ビットよりも広いマイクロプロセッサでも、レジスタの下位32ビットのみ使用することで同様の命令を導入することができる。

#### 【0132】

次に、本発明の第5の実施の形態について図面を参照して詳細に説明する。

#### 【0133】

図12は、本発明の第5の実施の形態の構成を示すブロック図である。

#### 【0134】

本発明の第5の実施の形態では、64ビット・レジスタを持つマイクロプロセッサに適用され、暗号化・復号化演算器を2重化し、レジスタの上位と下位で同時に演算することで、性能を約2倍にできる。

#### 【0135】

図12において、64ビット長の入力レジスタ1201（汎用レジスタに割り当てられる）は、 $b_i0 \sim b_i7$ までの8要素を保持する。図11の構成をAES処理命令向けの演算器コアとして多重化し（演算器コア1202、演算器コア1203）、上位4要素をひとつの演算器コア1202へ、下位4要素をもうひとつの演算器コア1203へ入力する。演算器コア1202、演算器コア1203の出力は連結され、64ビット長出力レジスタ1204（汎用レジスタに割り当てられる）へ格納される。

#### 【0136】

係数テーブル106と、行、暗号化・復号化を指定する即値とは、演算器コア1202、演算器コア1203で共用できる。64ビットより幅広のレジスタを持つマイクロプロセッサでも、同様の演算器コア多重化による性能拡張が可能である。入力レジスタ1201に置く複数のステートの列は、同一ステート内の異なる列でもよいし、別のステートの列でも構わない。

#### 【0137】

##### 【発明の効果】

本発明の効果は、AES暗号化および復号化に必要なテーブル容量を従来に比べ削減できることである。たとえば、非特許文献5（Gladmanの方法）では、暗号化と復号化を併せると64kビットのテーブルを必要としていた。

#### 【0138】

本発明では、2kビットのテーブル1個で暗号化、復号化の双方に対応しており、必要テーブル容量を1/32に削減できる。これはAES専用のアクセラレータや、マイクロプロセッサに専用AES命令を実装するための演算器が小面積で構成できることを示している。

#### 【0139】

さらに、マイクロプロセッサに本発明のAES演算器コアを使ったAES処理

専用命令を導入すれば外部メモリに置く S - b o x テーブルは不要になる。

【0140】

従って組み込み機器など外部メモリ容量に制限がある場合でも A E S 暗号化機能を組み込めるようになるという利点がある。外部メモリ容量に強い制限のないハイエンド機器においても、メモリ上のテーブルをアクセスする代わりに、A E S 処理専用命令を使えば、キャッシュ汚染を防ぎ高速化につながるという利点がある。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態の構成を示すブロック図である。

【図2】

図1の係数テーブルの内容を示す説明図である。

【図3】

本発明の第1の実施の形態の動作を示す説明図である。

【図4】

本発明の第2の実施の形態の構成を示すブロック図である。

【図5】

A E S 暗号化専用命令のニーモニック表記例を示す説明図である。

【図6】

入力レジスタ、出力レジスタのデータ配置を示す説明図である。

【図7】

A E S 暗号化命令の即値と出力との関係を示す説明図である。

【図8】

A E S \_ S S M 命令を含む命令列を示す説明図である。

【図9】

本発明の第3の実施の形態で使用する係数テーブルの内容を示す説明図である。

。

【図10】

A E S 複号化命令の即値と出力との関係を示す説明図である。

## 【図 1 1】

本発明の第 4 の実施の形態の構成を示すブロック図である。

## 【図 1 2】

本発明の第 5 の実施の形態の構成を示すブロック図である。

## 【図 1 3】

$GF(2^8)$  上の加算器の例を示すブロック図である。

## 【図 1 4】

$GF(2^8)$  上の 2 倍回路の例を示すブロック図である。

## 【図 1 5】

$GF(2^8)$  上のガロア体乗算器の例を示すブロック図である。

## 【図 1 6】

図 1 の S - b o x テーブルの内容を示す説明図である。

## 【図 1 7】

I n v e r s e S - b o x の内容を示す説明図である。

## 【図 1 8】

逆アフィン変換回路の内容を示す説明図である。

## 【図 1 9】

逆数テーブルの内容を示す説明図である。

## 【図 2 0】

アフィン変換回路の内容を示す説明図である。

## 【図 2 1】

A E S 暗号のデータ構造であるステートを示す説明図である。

## 【図 2 2】

A E S 暗号化の手順を示すフローチャートである。

## 【図 2 3】

A E S 暗号化のラウンド処理の一部を示すシグナルフローである。

## 【図 2 4】

従来の非特許文献 4 (M c L o o n e ら) の高速化手法を示すシグナルフローである。

## 【図 2 5】

非特許文献 5 の高速化手法を示すシグナルフローである。

## 【図 2 6】

A E S 復号化の手順を示すフローチャートである。

## 【符号の説明】

- 1 0 1     入力ステート
- 1 0 2     列マルチプレクサ
- 1 0 3     演算入力レジスタ
- 1 0 4     行マルチプレクサ
- 1 0 5     S - b o x テーブル
- 1 0 6     係数テーブル
- 1 0 7     ガロア体乗算器
- 1 0 8     演算結果レジスタ
- 1 0 9     ガロア体加算器
- 1 1 0     累算レジスタ
- 1 1 1     A E S 暗号回路
- 4 0 1     汎用レジスタ群
- 4 0 2     命令バッファ
- 4 0 3     デコーダ
- 4 0 4     補助レジスタ
- 4 0 5     補助レジスタ
- 4 0 6     補助レジスタ
- 4 0 7     補助レジスタ
- 4 0 8     補助レジスタ
- 4 0 9     補助レジスタ
- 4 1 0     汎用演算回路
- 4 1 1     演算結果レジスタ
- 4 1 2     書き込みマルチプレクサ
- 1 1 0 1     逆アフィン変換回路

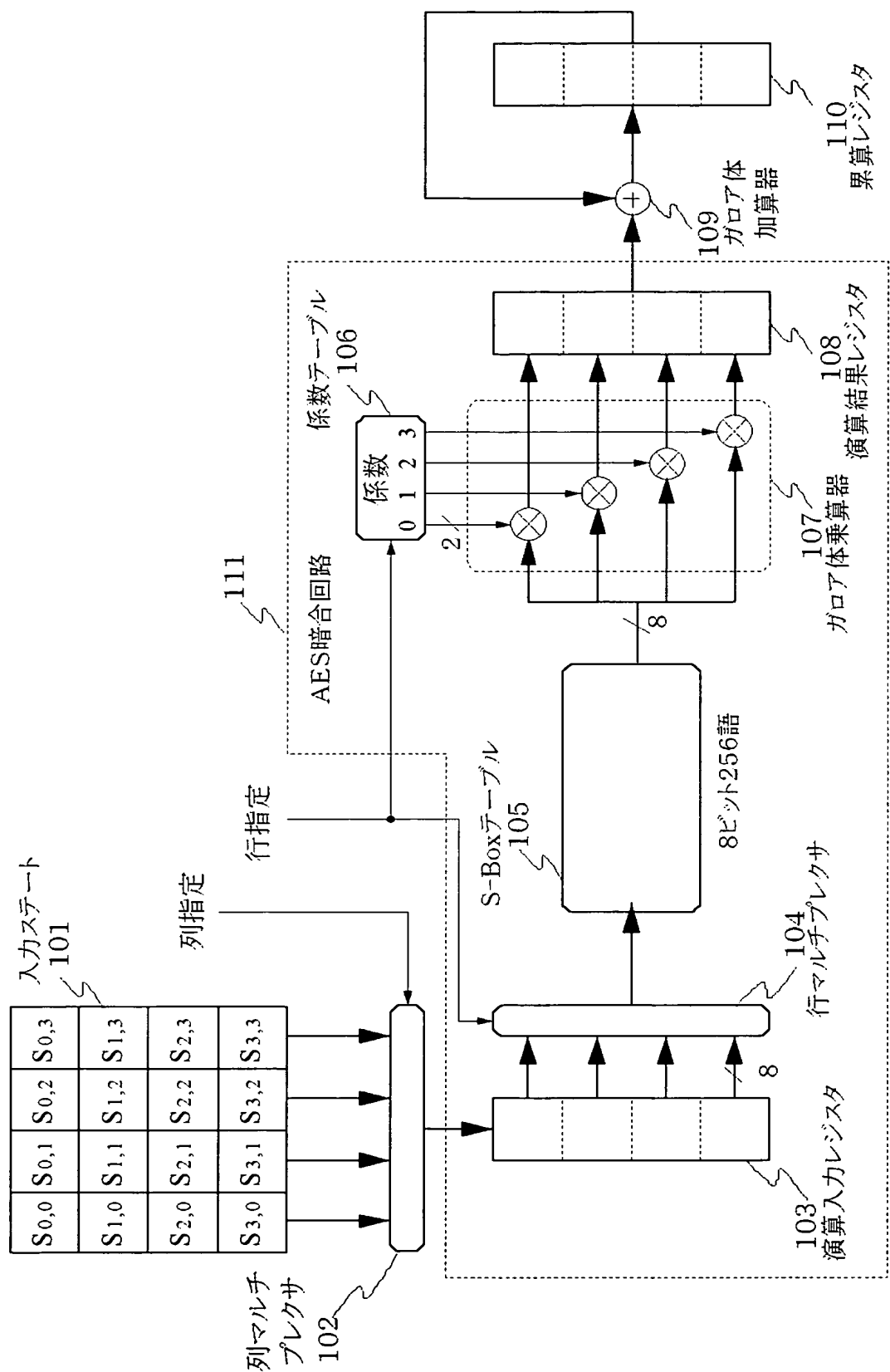
- 1 1 0 2 暗号化マルチプレクサ
- 1 1 0 3 逆数テーブル
- 1 1 0 4 アフィン変換回路
- 1 1 0 5 暗号化マルチプレクサ
- 1 2 0 1 入力レジスタ
- 1 2 0 2 演算器コア
- 1 2 0 3 演算器コア
- 1 2 0 4 出力レジスタ



【書類名】

図面

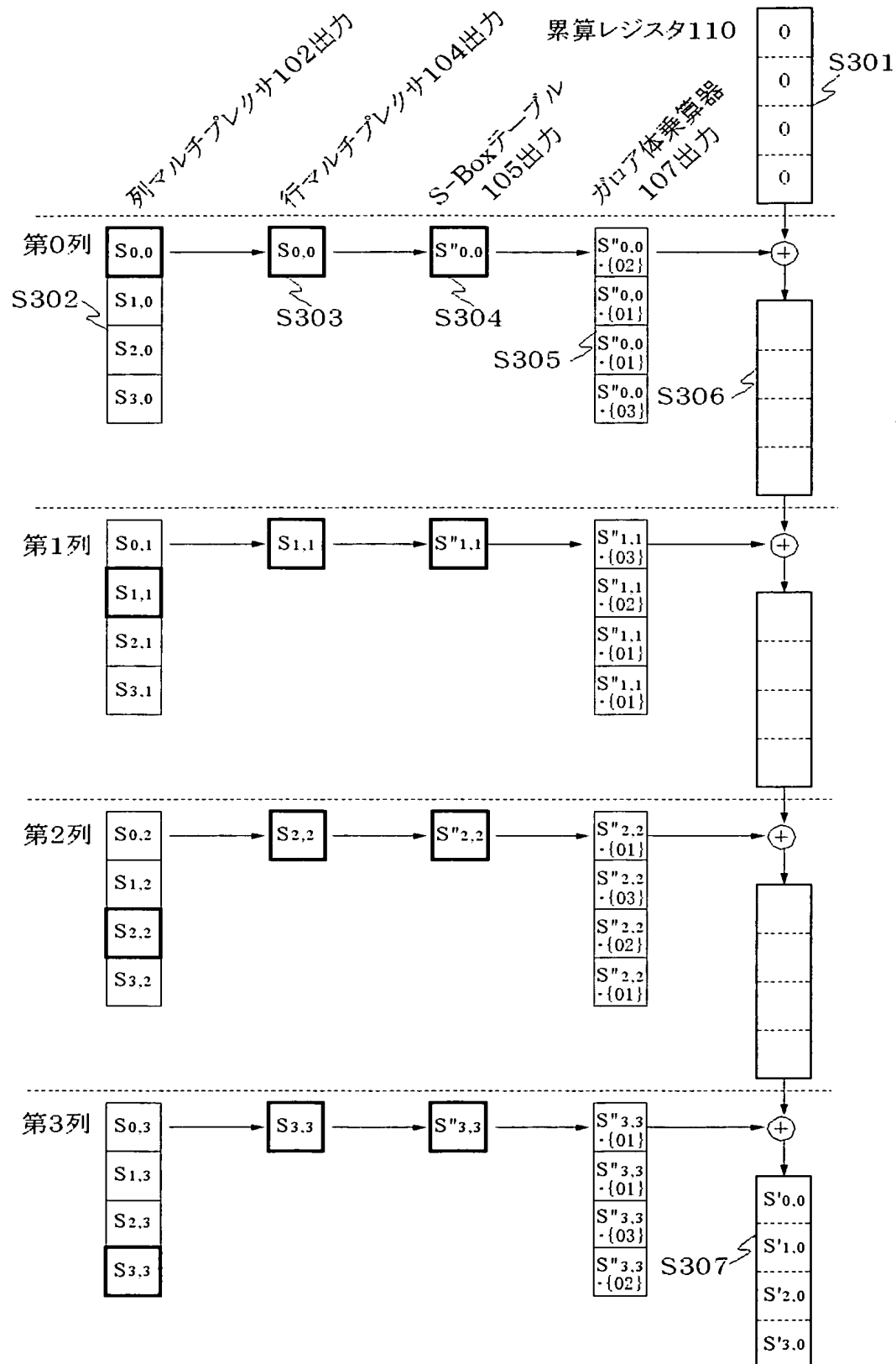
【図 1】



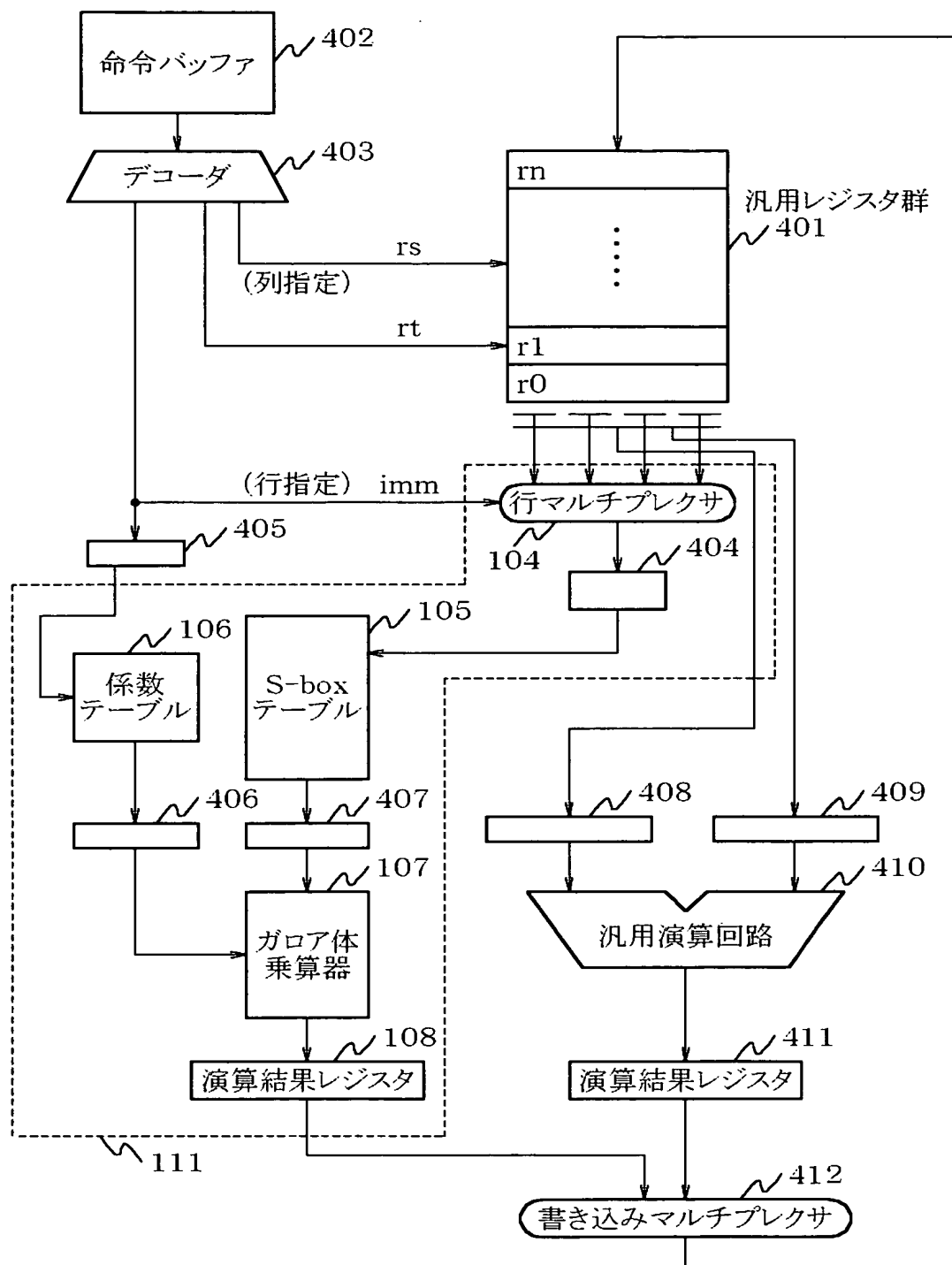
【図 2】

行指定	係数テーブル出力			
	係数3	係数2	係数1	係数0
0	{02}	{01}	{01}	{03}
1	{03}	{02}	{01}	{01}
2	{01}	{03}	{02}	{01}
3	{01}	{01}	{03}	{02}

【図 3】



【図 4】



【図 5】

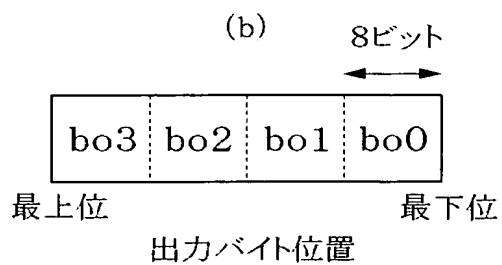
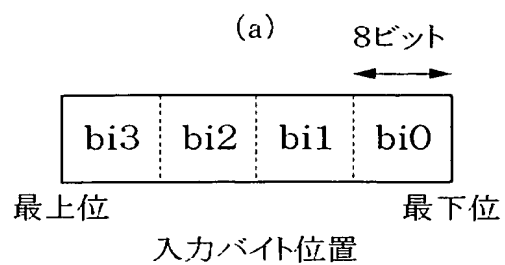
AES\_SSM rs, rt, imm

rs: 入力レジスタ

rt: 出力レジスタ

imm: 即値

【図 6】



【図 7】

入力即値	出力			
行指定	bo3	bo2	bo1	bo0
00	S-box (bi0)・{02}	S-box (bi0)・{01}	S-box (bi0)・{01}	S-box (bi0)・{03}
01	S-box (bi1)・{03}	S-box (bi1)・{02}	S-box (bi1)・{01}	S-box (bi1)・{01}
02	S-box (bi2)・{01}	S-box (bi2)・{03}	S-box (bi2)・{02}	S-box (bi2)・{01}
03	S-box (bi3)・{01}	S-box (bi3)・{01}	S-box (bi3)・{03}	S-box (bi3)・{02}

【図 8】

```

; 入力:
; r0=[S3,0 S2,0 S1,0 S0,0]
; r1=[S3,1 S2,1 S1,1 S0,1]
; r2=[S3,2 S2,2 S1,2 S0,2]
; r3=[S3,3 S2,3 S1,3 S0,3]
;
; 作業用レジスタ:r4
; 累算レジスタ:r5
;
; 出力:
; r5=[S'3,0 S'2,0 S'1,0 S'0,0]
;
AES_SSM r0, r5, 0 ; S0,0 = r0, bi0
AES_SSM r1, r4, 1 ; S1,1 = r1, bi1
XOR      r5, r4, r5 ; r5 = r5 XOR r4
AES_SSM r2, r4, 2 ; S2,2 = r2, bi2
XOR      r5, r4, r5 ; r5 = r5 XOR r4
AES_SSM r3, r4, 3 ; S3,3 = r3, bi3
XOR      r5, r4, r5 ; r5 = r5 XOR r4

```

【図 9】

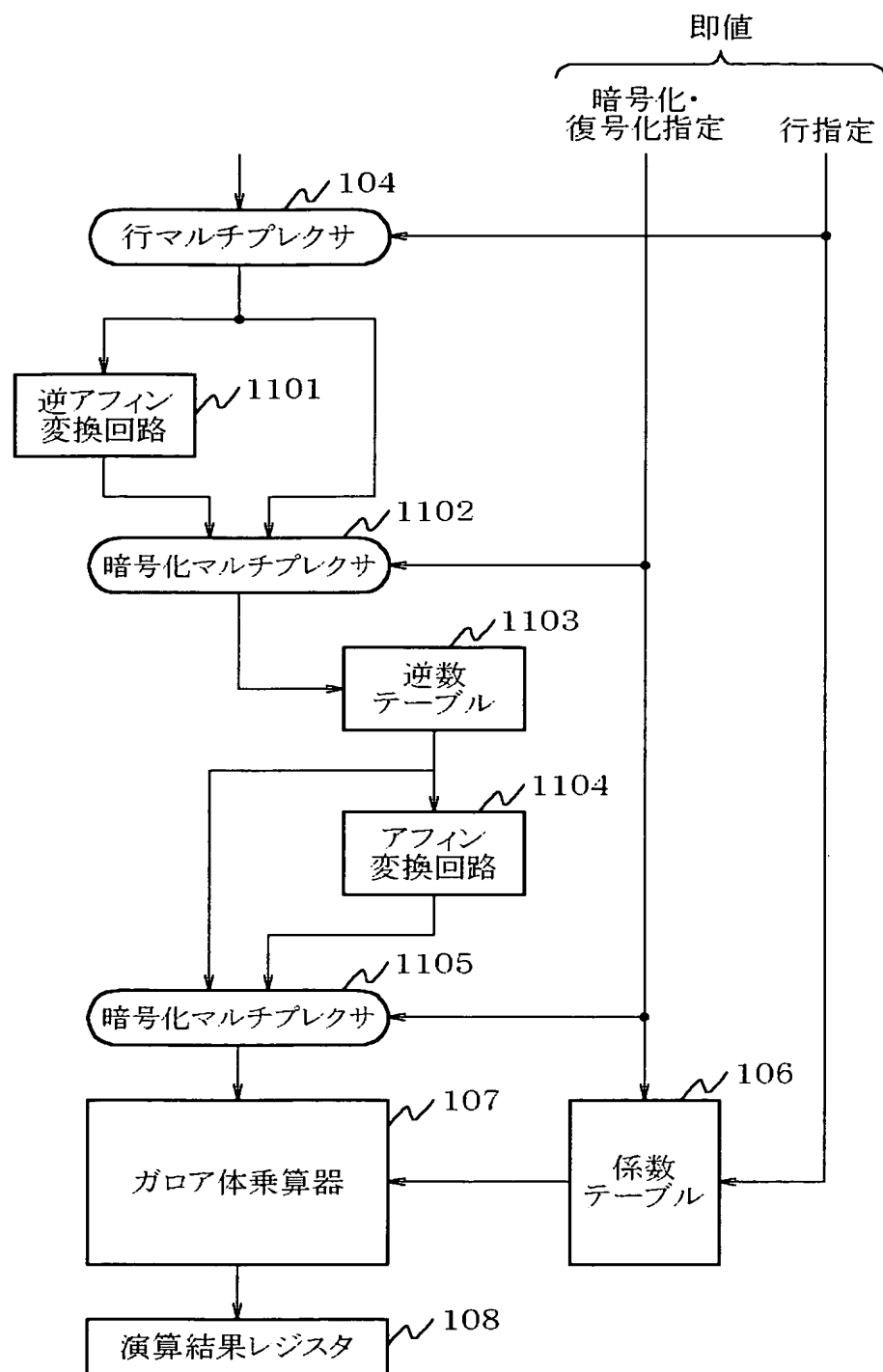
行指定	係数テーブル出力			
	係数3	係数2	係数1	係数0
0	{0e}	{09}	{0d}	{0b}
1	{0b}	{0e}	{09}	{0d}
2	{0d}	{0b}	{0e}	{09}
3	{09}	{0d}	{0b}	{0e}



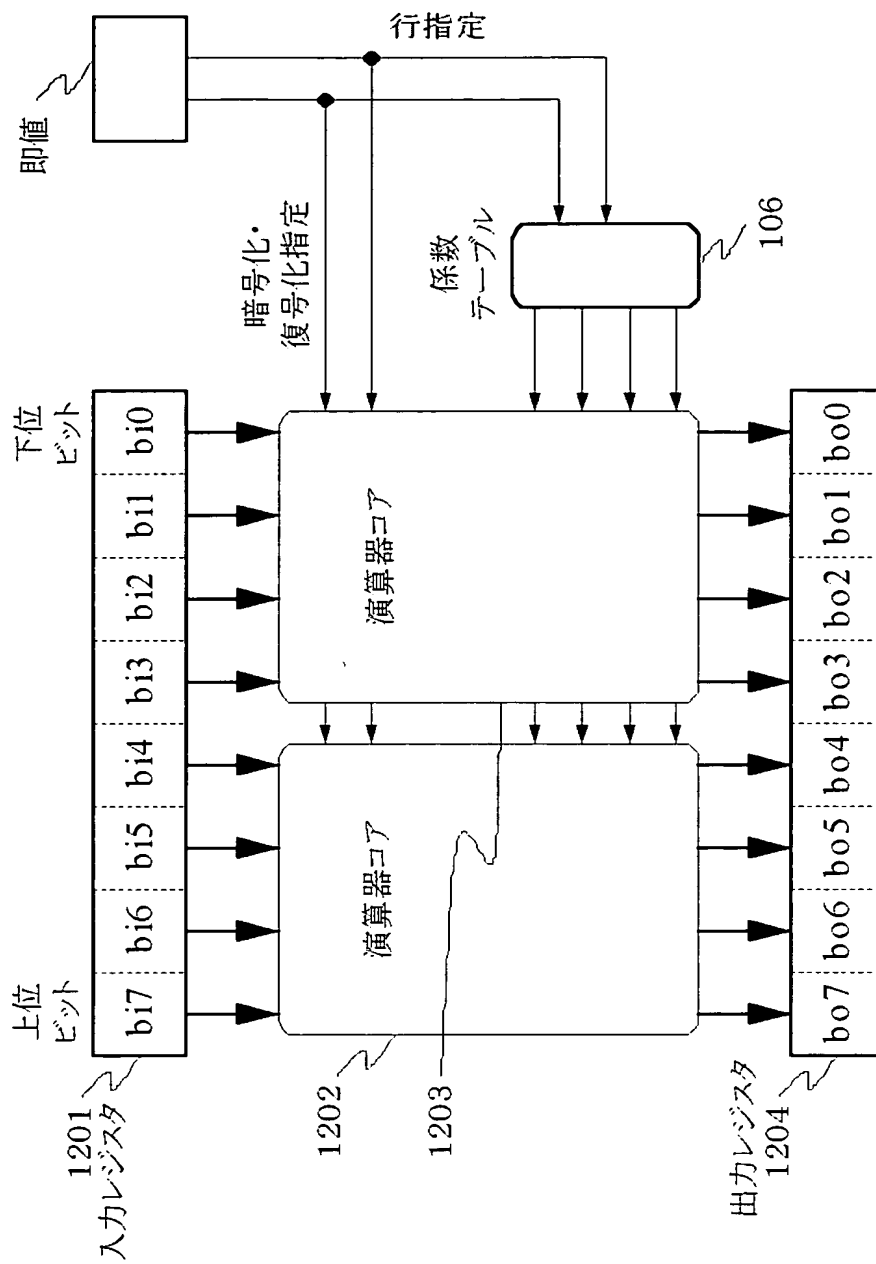
【図 1 0】

入力即値	出力			
行指定	bo3	bo2	bo1	bo0
00	InvS-box (bi0)・{0e}	InvS-box (bi0)・{09}	InvS-box (bi0)・{0d}	InvS-box (bi0)・{0b}
01	InvS-box (bi1)・{0b}	InvS-box (bi1)・{0e}	InvS-box (bi1)・{09}	InvS-box (bi1)・{0d}
02	InvS-box (bi2)・{0d}	InvS-box (bi2)・{0b}	InvS-box (bi2)・{0e}	InvS-box (bi2)・{09}
03	InvS-box (bi3)・{09}	InvS-box (bi3)・{0d}	InvS-box (bi3)・{0b}	InvS-box (bi3)・{0e}

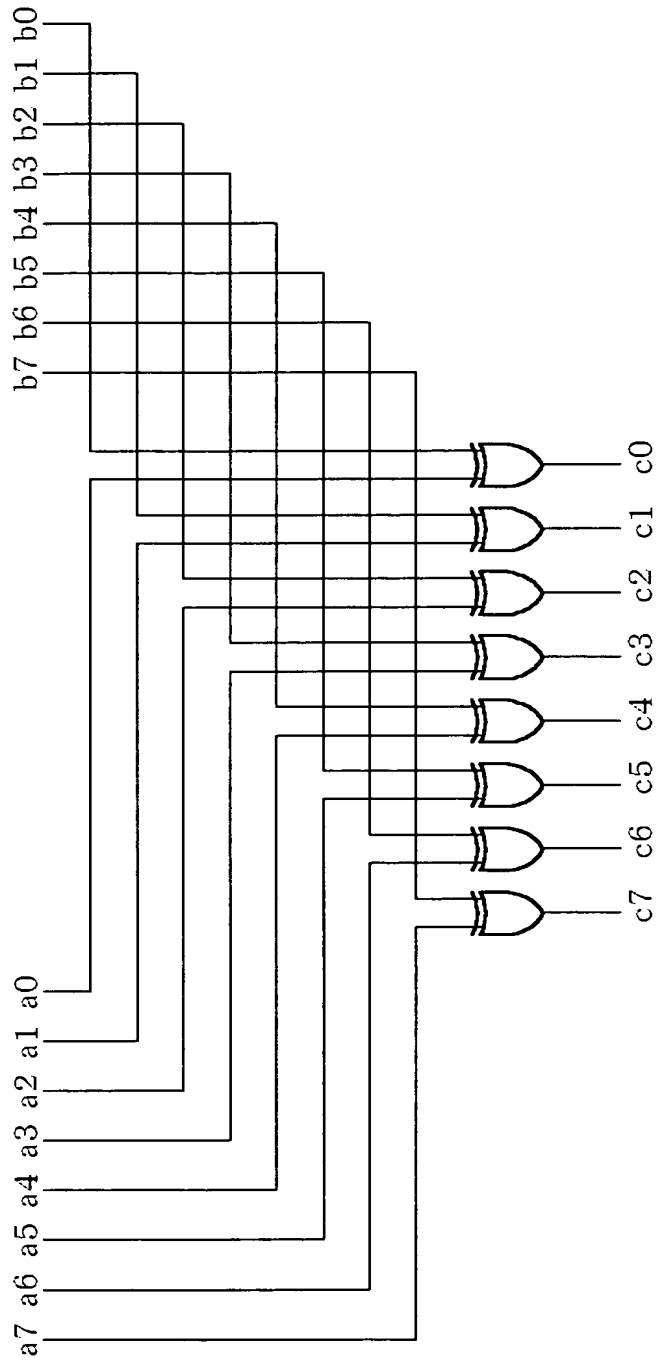
【図 11】



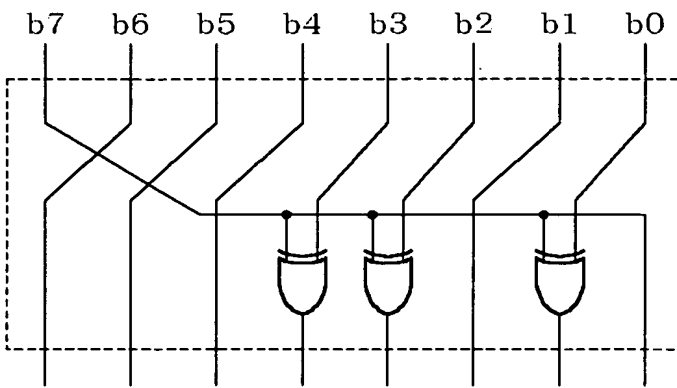
【図 12】



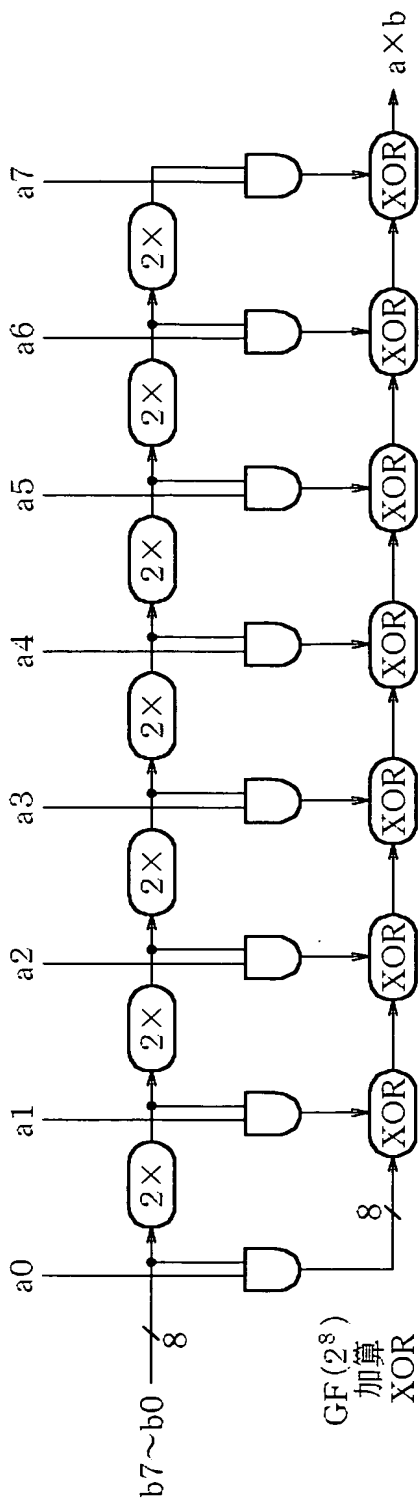
【図 13】



【図 14】



【図 15】



【図 16】

		下位																
		y																
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
上位	x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
		1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
		2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
		3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
		4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
		5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
		6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
		7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
		8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
		9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
		a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
		b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
		c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
		d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
		e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
		f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

【図 17】

		下位																
		y																
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
上位	x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
		1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
		2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
		3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
		4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
		5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
		6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
		7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
		8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
		9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
		a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
		b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
		c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
		d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
		e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
		f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

【図 18】

$$b'_i = b_{(i+2) \bmod 8} \langle \text{XOR} \rangle b_{(i+5) \bmod 8} \langle \text{XOR} \rangle b_{(i+7) \bmod 8} \langle \text{XOR} \rangle c_i$$

【図 19】

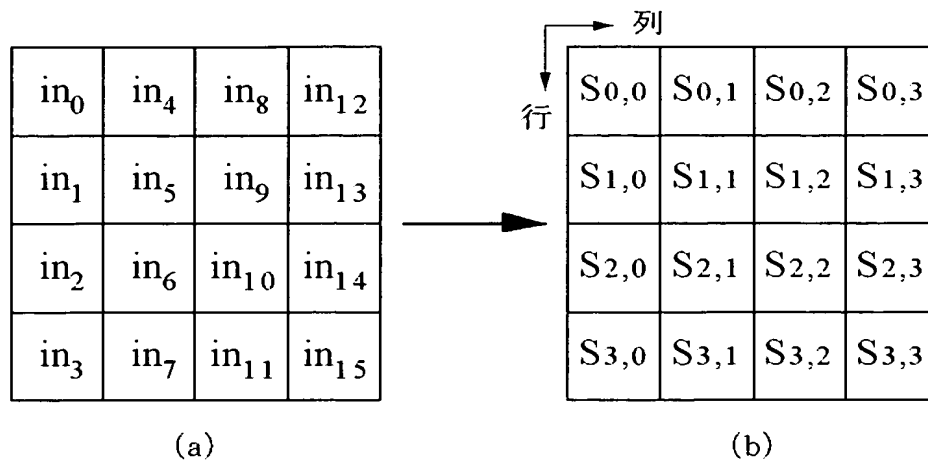
		下位																
		y																
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
上位	x	0	00	01	8d	f6	cb	52	7b	d1	e8	4f	29	c0	b0	e1	e5	c7
	1	74	b4	aa	4b	99	2b	60	5f	58	3f	fd	cc	ff	40	ee	b2	
	2	3a	6e	5a	f1	55	4d	a8	c9	c1	0a	98	15	30	44	a2	c2	
	3	2c	45	92	6c	f3	39	66	42	f2	35	20	6f	77	bb	59	19	
	4	1d	fe	37	67	2d	31	f5	69	a7	64	ab	13	54	25	e9	09	
	5	ed	5c	05	ca	4c	24	87	bf	18	3e	22	f0	51	ec	61	17	
	6	16	5e	af	d3	49	a6	36	43	f4	47	91	df	33	93	21	3b	
	7	79	b7	97	85	10	b5	ba	3c	b6	70	d0	06	a1	fa	81	82	
	8	83	7e	7f	80	96	73	be	56	9b	9e	95	d9	f7	02	b9	a4	
	9	de	6a	32	6d	d8	8a	84	72	2a	14	9f	88	f9	dc	89	9a	
	a	fb	7c	2e	c3	8f	b8	65	48	26	c8	12	4a	ce	e7	d2	62	
	b	0c	e0	1f	ef	11	75	78	71	a5	8e	76	3d	bd	bc	86	57	
	c	0b	28	2f	a3	da	d4	e4	0f	a9	27	53	04	1b	fc	ac	e6	
	d	7a	07	ae	63	c5	db	e2	ea	94	8b	c4	d5	9d	f8	90	6b	
	e	b1	0d	d6	eb	c6	0e	cf	ad	08	4e	d7	e3	5d	50	1e	b3	
	f	5b	23	38	34	68	46	03	8c	dd	9c	7d	a0	cd	1a	41	1c	



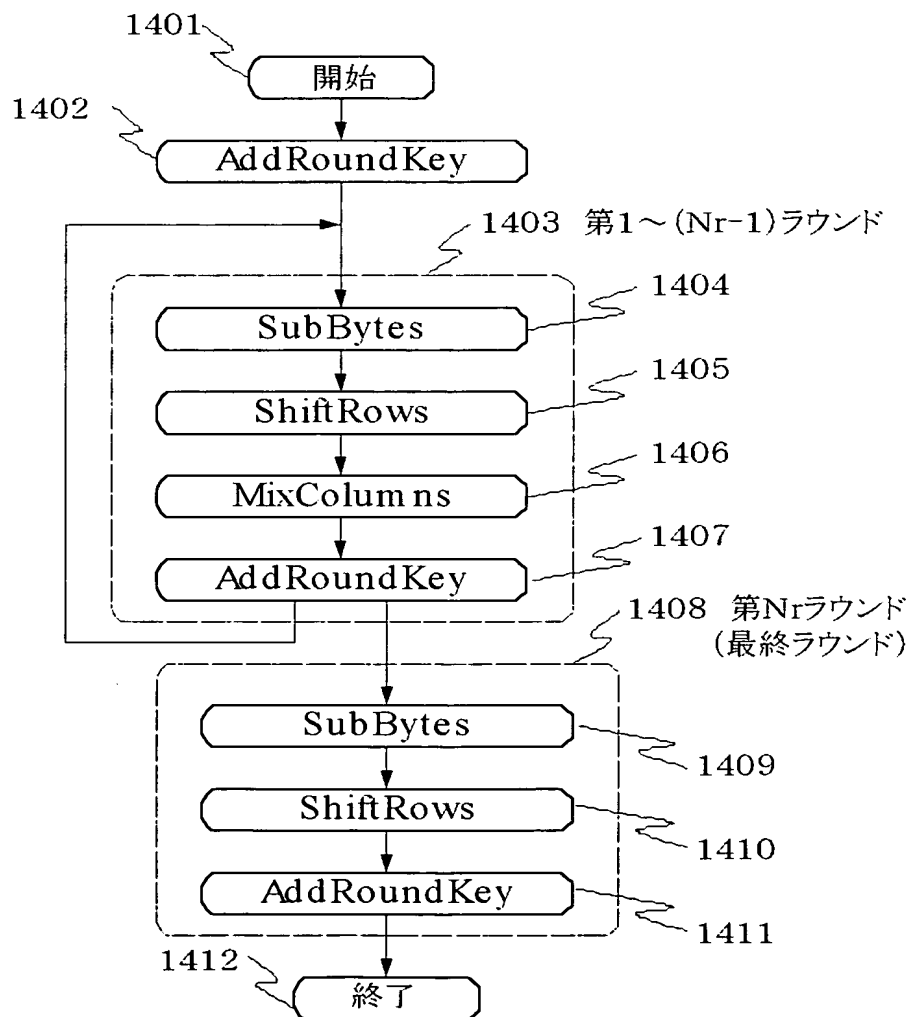
【図 2 0】

$$b'_i = b_i \langle \text{XOR} \rangle b_{(i+4) \bmod 8} \langle \text{XOR} \rangle b_{(i+5) \bmod 8} \langle \text{XOR} \rangle b_{(i+6) \bmod 8} \langle \text{XOR} \rangle b_{(i+7) \bmod 8} \langle \text{XOR} \rangle c_i$$

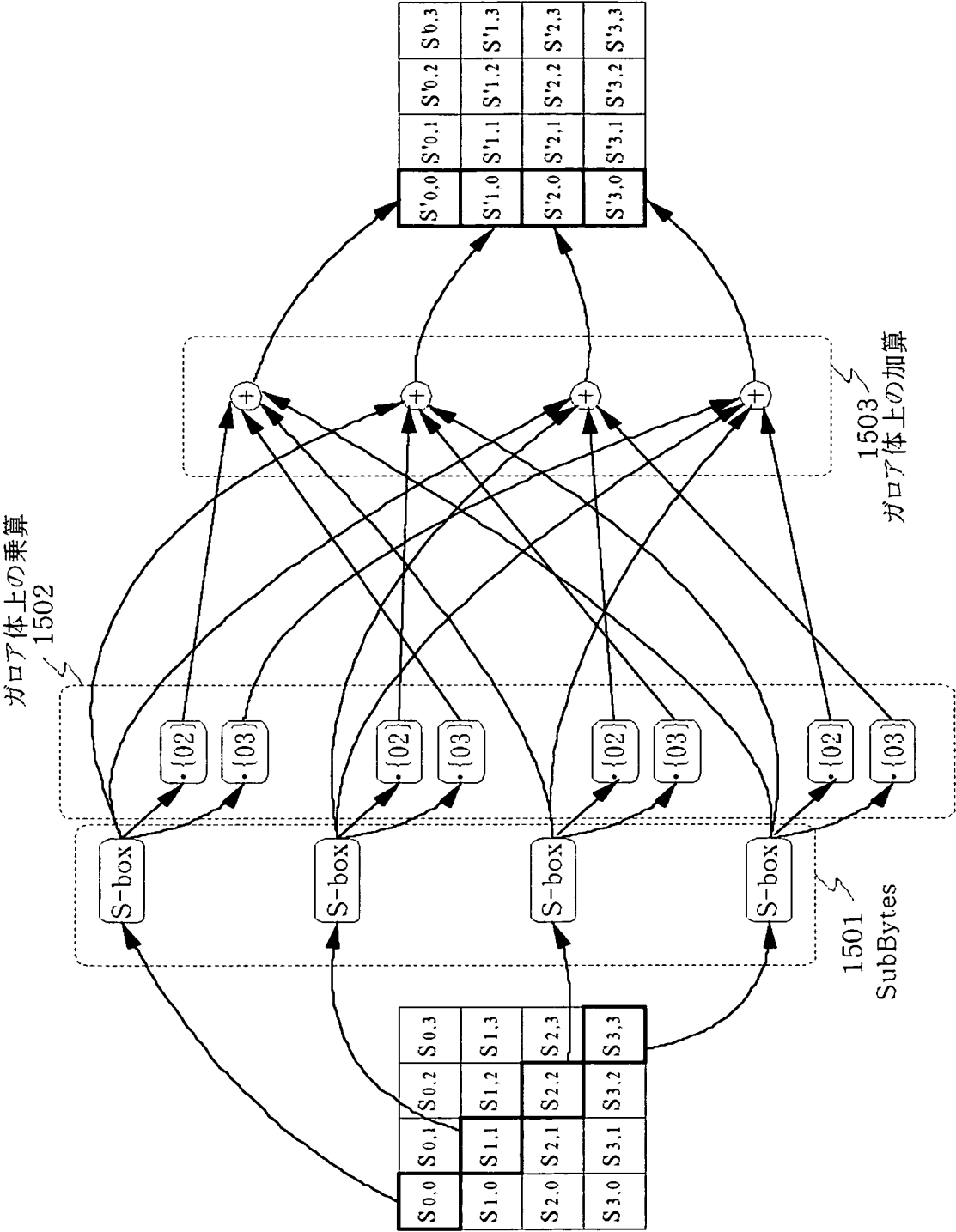
【図21】



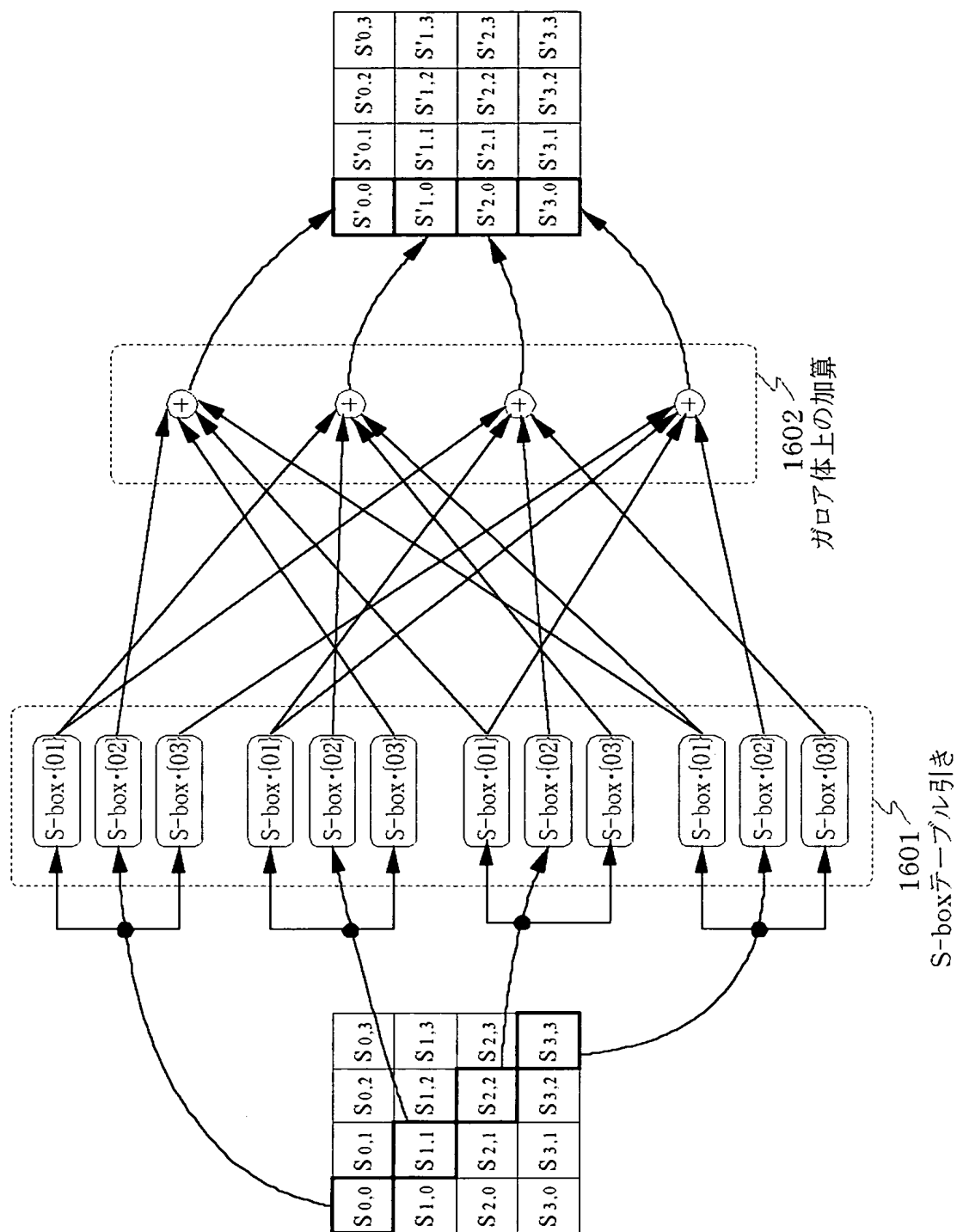
【図22】



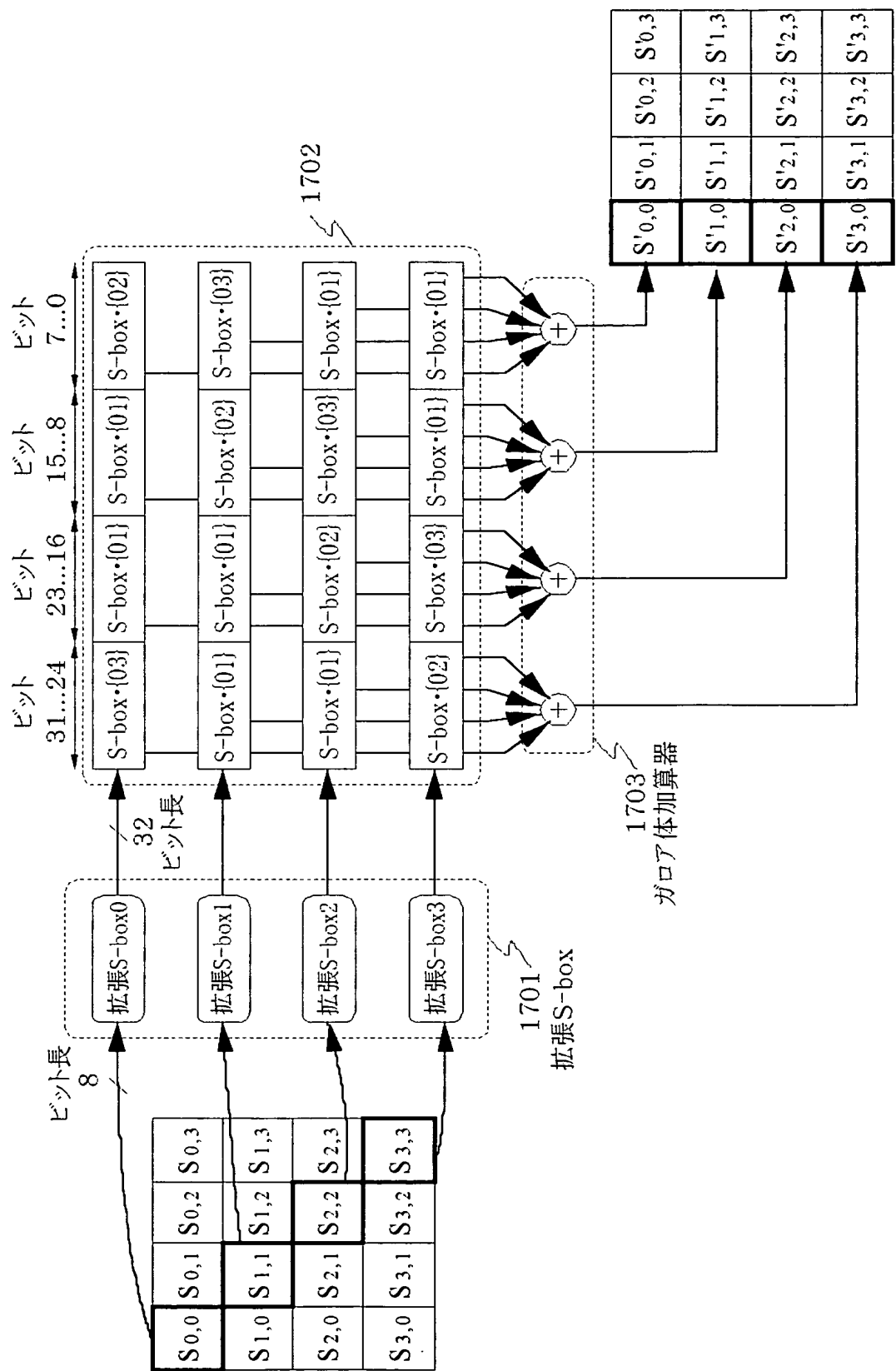
【図23】



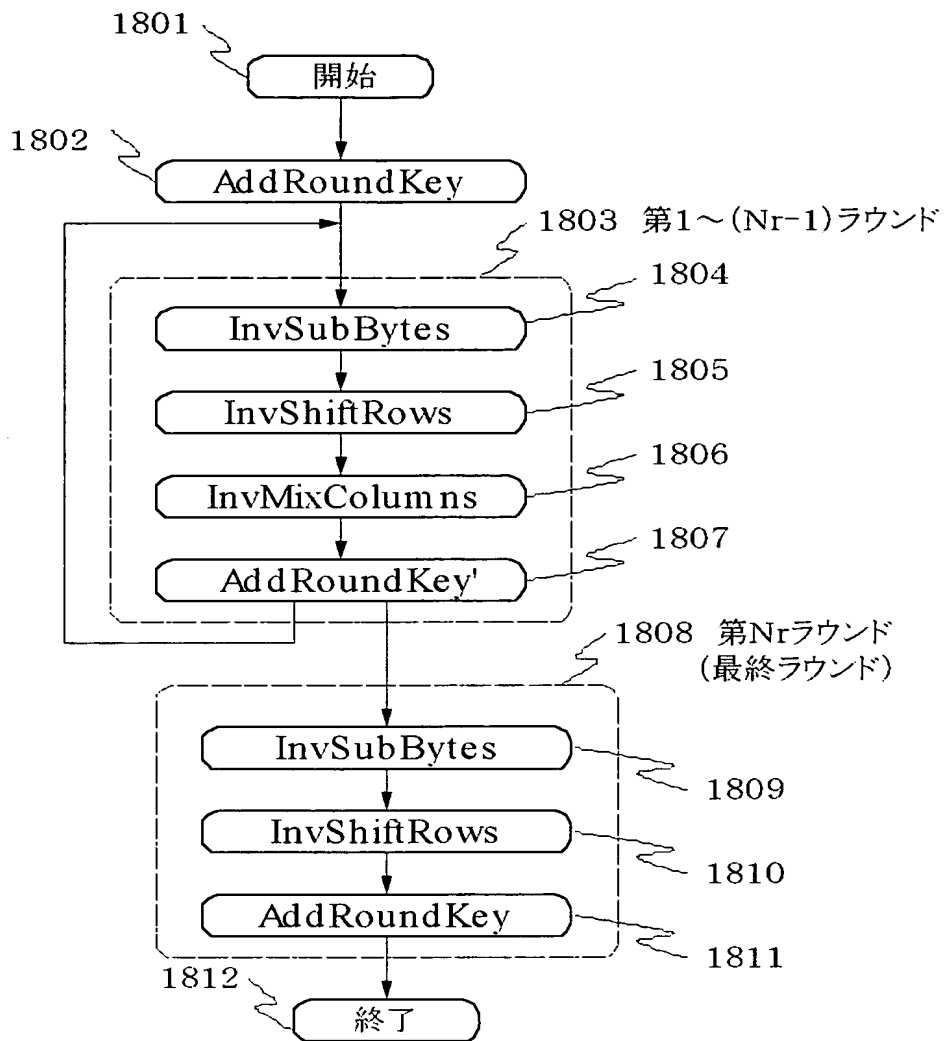
【図 24】



【図 25】



【図 26】



【書類名】 要約書

【要約】

【課題】 AES暗号処理回路の性能を保ちつつ、換字テーブル（S-box）の容量を削減する。

【解決手段】 列マルチプレクサ102、行マルチプレクサ104により、入力ステート101上の8ビットの1要素が選択される。選択された要素は、S-boxテーブル105により換字処理され、ガロア体乗算器107に入力される。ガロア体乗算器107により、S-boxテーブル105の出力と係数テーブル106出力とを4並列乗算し、32ビット出力を演算結果レジスタ108に格納する。演算結果レジスタ108の出力は、ガロア体加算器109により、累算レジスタ110と加算され累算レジスタ110に格納される。

【選択図】 図1

## 認定・付加情報

特許出願の番号	特願 2003-018845
受付番号	50300132487
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 1月29日

## &lt; 認定情報・付加情報 &gt;

【提出日】	平成15年 1月28日
-------	-------------

次頁無



特願 2 0 0 3 - 0 1 8 8 4 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 4 2 3 7 ]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社